# Department of Homeland Security
# Office of Inspector General

## Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports (Redacted)

OIG-12-80

May 2012

*Office of Inspector General*

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

May 3, 2012

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 is prepared in response to Senator Frank Lautenberg's request for an investigation into media reports focused on security breaches at Newark Liberty International Airport, including the contributing factors that led to the security breaches. 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.

Anne L Richards
Anne L. Richards
Assistant Inspector General for Audits

# Table of Contents/Abbreviations

## Appendices

## Abbreviations

| | |
|---|---|
| DHS | Department of Homeland Security |
| EWR | Newark Liberty International Airport |
| FSD | Federal Security Director |
| OIG | Office of Inspector General |
| PARIS | Performance and Results Information System |
| SOP | Standard Operating Procedures |
| TSA | Transportation Security Administration |
| TSO | Transportation Security Officer |
| TSOC | Transportation Security Operations Center |

[redacted]

OIG

*Department of Homeland Security*
*Office of Inspector General*

## Executive Summary

Senator Frank Lautenberg requested an investigation into media reports focused on security breaches at Newark Liberty International Airport, including the contributing factors that led to the security breaches. He requested that we compare the incident rate of breaches at Newark to other airports in the region and comparable airports. He asked us to determine whether corrective action had been taken on the specific security incidents. We determined whether the Transportation Security Administration (TSA) at Newark had more security breaches than at other airports. We also determined whether TSA has an effective mechanism to use the information gathered from individual airports to identify measures that could be used to improve security nationwide.

Of the six airports we reviewed, TSA at Newark [redacted] Our analysis showed that TSA at Newark has taken corrective actions to address the incidents identified by Senator Lautenberg, but took corrective actions for only 42% of the security breaches shown in its records.

While TSA has several programs and initiatives that report and track identified security breaches, TSA does not have a comprehensive oversight program in place to gather information about all security breaches and therefore cannot use the information to monitor trends or make general improvements to security. The agency does not provide the necessary guidance and oversight to ensure that all breaches are consistently reported, tracked, and corrected. As a result, it does not have a complete understanding of breaches occurring at the Nation's airports and misses opportunities to strengthen aviation security. TSA concurred with both our recommendations.

## Background

Newark Liberty International Airport (Newark or EWR) is located 14 miles from Manhattan and serves an important role for the New York/New Jersey metropolitan area. In 2010, approximately 33 million people traveled through Newark Liberty International Airport, making it one of the country's busiest airports.

Senator Frank Lautenberg requested an investigation into security breaches reported by the media at Newark. A string of security breaches at the airport heightened concern regarding safety and security. These security breaches included a man gaining access to the sterile area of a terminal, shutting down operations for 6 hours; and a dead dog being placed on a passenger plane without the proper screening.

Senator Lautenberg asked the Department of Homeland Security (DHS) Office of Inspector General (OIG) to review the contributing factors that led to the security breaches, the TSA's response to the breaches, and the general level of security at the airport. He also requested that we compare the incident rate of breaches at Newark to other airports in the New Jersey/New York region and comparable airports nationwide. The Senator's letter is in appendix C.

There are varying levels and definitions of security breaches. For purposes of this audit, a "security breach" is an individual or individuals gaining access to the sterile area, specifically at the checkpoint or exit lane, without submitting to all screening, inspections, and detection according to TSA's Standard Operating Procedures (SOP). For instance, a person entering the sterile area by sneaking through an exit lane without anyone preventing the entry would be considered a security breach for this report.

Newark airport operations are managed by the airport authority, airline personnel, law enforcement officials, and other government agencies. TSA at the airport coordinates with these stakeholders to assist in the prevention and mitigation of security breaches. In the event of a security breach, these stakeholders may be involved in evacuating the terminals, suspending arriving flights, preventing the boarding of departing flights, and assisting TSA.

TSA at Newark is composed of a Federal Security Director (FSD), one Deputy FSD, two Deputy Assistant FSDs, several Assistant FSDs, managers, and approximately 943 Transportation Security Officers (TSOs). Appendix D illustrates the expected process for identifying, reporting, and tracking security breaches.

Security breaches are documented locally by TSA at each airport. TSA staff is required to report security breaches through TSA's Performance and Results Information System (PARIS) and the Transportation Security Operations Center (TSOC). The TSOC is expected to use this information to identify events occurring at disparate locations throughout the U.S. transportation system that could represent an orchestrated attempt to defeat or circumvent security protocols. We did not evaluate how the TSOC used the information about the security breaches we reviewed.

PARIS is TSA's internal reporting system and official record of a security incident. As detailed in appendix F, PARIS contains 33 categories of possible incidents. For this audit, we focused on incident reports in three PARIS categories:

- Security breaches,
- Improper/no screening, and
- Sterile area security events.

These categories are defined as security breaches because they include an individual or individuals gaining access to the sterile area through a checkpoint or exit lane without submitting to all screening, inspections, and detection according to TSA's SOP.

# Results of Audit

Of the six airports we reviewed, Newark [redacted] Our analysis showed that TSA at Newark has taken corrective actions to address each of the incidents identified by Senator Lautenberg, but took corrective actions for only 42% of the security breaches shown in their records. TSA has taken steps to improve operations at Newark, including a "Back to Basics" campaign to reinforce procedures and a study of identified shortcomings and potential solutions entitled Newark Commitment to Excellence.

According to TSA, there are many programs and initiatives to report and track security breaches identified. TSA reports that it collects thousands of records of incidents and security breaches occurring at airports and other transportation facilities. However, TSA does not have a comprehensive mechanism in place to gather and track all security breaches. The agency cannot use this information to monitor trends or make general improvements to security. TSA does not provide the necessary guidance and oversight to ensure that all breaches are consistently reported, tracked, and corrected. As a result, it does not have a complete understanding of breaches occurring at the Nation's airports and misses opportunities to strengthen aviation security.

## TSA's Efforts at Newark Liberty International Airport

[redacted]

We reviewed actual security breach incident report files from Newark and five comparable airports dated January 1, 2010, to May 31, 2011. Our review showed that the number of security breaches (security breaches, improper/no screening, and sterile area security events) in Newark during the 17-month period was slightly higher than [redacted] (see figure 1).

**Figure 1: Security Breach File Reviews at Six Category X[1] Airports Between January 1, 2010, and May 31, 2011**

[redacted]

Although Newark's [redacted] security breaches [redacted] among the other airports reviewed, the types of breaches were similar. These breaches included TSOs not detecting prohibited items (e.g., knives) in carry-on baggage or not conducting the required additional screening of passengers who were identified as selectees.

## Corrective Actions Were Taken To Address Only Some Incidents at Newark

Newark took or documented actions to correct only [redacted] (42%) of the [redacted] security breach vulnerabilities identified during the incident report file review. Most of the security breaches in which corrective action was not taken occurred in 2010. Since 2010, Newark has improved efforts to correct security breach vulnerabilities.

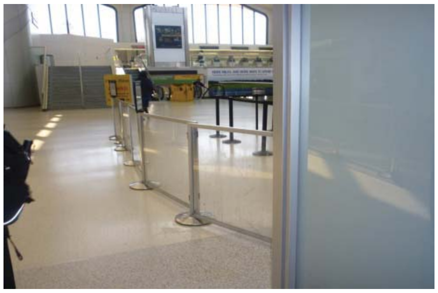
[1] This includes security breaches, sterile area access events, and improper/no screening. Category X airports are the Nation's largest and busiest airports as measured by the volume of passenger traffic and may be attractive targets for criminal and terrorist activity.

We verified that Newark implemented corrective actions to address each of the incidents cited in Senator Lautenberg's letter.  These actions included a civil penalty, letters of reprimand or suspension for TSOs, and repairing an accessible gate.  Table 1 explains the actions taken to correct each of the incidents occurring between January and February 2011, as identified by Senator Lautenberg.

**Table 1:  Actions Taken To Address Incidents at Newark**

| Date | Security Breach | Actions Taken to Address Incidents |
|---|---|---|
| 1/4/2011 | A dead dog was loaded on a departing flight without screening for explosives or disease. | A civil penalty of $55,000 against the airline is pending. |
| 1/16/2011 | A carry-on bag containing a knife bypassed TSA screening. | The TSO received a 5-day suspension for not following the SOP. |
| 1/30/2011 | A TSO handled a bag improperly after it was x-rayed. | The TSO received a Letter of Reprimand. |
| 2/1/2011 | A passenger bypassed TSA screening by walking through a disability gate. | The TSO received a 3-day suspension for leaving her position at the accessible gate. Letters of Reprimand were issued to the Supervisory TSOs involved for failing to follow breach procedures and inattention to duties. TSA had a maintenance team repair the latch on the accessible gate. |
| 2/3/2011 | Two passengers were allowed through screening even though the monitor on a full-body scanner had malfunctioned. | The TSO received a Letter of Reprimand for failing to follow the SOP. |
| 2/21/2011 | A passenger was not screened properly and entered the sterile area. | TSA took no action.  However, The TSOs involved received a Notice of Breach of Rules from Port Authority Police Department for failing to conduct proper screening and following Advanced Imaging Technology procedures. |

**Figure 2: Glass Partitions at Newark Liberty International Airport**



**Source: DHS OIG**

TSA at Newark has also implemented actions to correct several vulnerabilities associated with other security breaches. For example, Newark replaced rope lanes with glass partitions after a man entered the sterile area through the exit lane in January 2010 (see figure 2).

TSA management collaborated with the workforce to review security procedures and best practices at Newark and several other airports. As a result, in April 2011 TSA issued the report *Newark Commitment to Excellence*, which identified shortcomings and proposed solutions to perceived areas of weakness. These proposals include enhancing employee training to include mandated follow-up training and instituting a program of targeted training for Lead TSOs. This should help ensure that frontline officers have the skills necessary to effectively direct screening, respond to incidents, and prevent them from occurring.

TSA at Newark also implemented a “Back to Basics” campaign to reinforce passenger and baggage screening procedures among the workforce. This campaign promoted the increased management and supervisory review of operations to ensure that employees follow procedures.

Other actions taken at the airport include addressing checkpoint vulnerabilities and actions against employees and responsible parties for violating procedures, such as disciplinary actions and civil penalties. TSA at Newark has taken steps to ensure the isolation of carry-on bags that have been flagged for further screening, which has been the cause of security events at Newark and other airports we visited. TSA at the airport has also promoted the effective use of closed-circuit television.

### Newark Has Controls To Prevent, Minimize, Respond to, and Correct Breaches

TSA at Newark has various controls in place to prevent, minimize, respond to, and correct security breaches. These controls include the following:

- Personnel to test the TSO workforce on checkpoint practices to ensure compliance with the SOP;
- Staffing exit lanes with two TSOs;
- Development of a Security Breach Containment Plan designed to outline procedures to follow when a security breach occurs;
- Meetings to determine the cause and actions needed to correct breach vulnerabilities; and
- Remedial training or disciplinary action for TSOs who do not follow the SOP.

See appendix E for more examples of controls and promising practices at Newark and at the other airports we visited.

## TSA's Guidance and Oversight for Reporting Breaches Nationwide

According to TSA, the agency has many programs and initiatives that report and track identified security breaches. TSA reports that it collects thousands of records of incidents and security breaches occurring at airports and other transportation facilities. However, TSA does not have a centralized mechanism in place to consolidate information about all security breaches and therefore cannot use information collected to monitor trends or make general improvements to security. Specifically, local TSA airport employees do not always properly report, track, and analyze all security breaches in PARIS. At the six airports visited, TSA did not always take action or document their actions to correct security breach vulnerabilities, because the agency did not provide TSA management at the airports with a clear definition or guidance for identifying and reporting security breaches through its reporting systems. Also, TSA did not provide oversight to ensure that all security breaches are consistently reported, tracked, and corrected.

## TSA Efforts to Improve Breach Data Collection and Analysis

According to TSA, there are many programs and initiatives that report and track identified security breaches. However, the various activities tracked are not all inclusive or centrally managed. TSA reports that it collects thousands of records of incidents and security breaches occurring at airports and other transportation facilities. The agency documents and disseminates the information to the program offices through various channels of reporting. These channels include:

- The Transportation Security Operations Center—this is the nerve center for TSA's operational control of crises and incidents and is the security incident information conduit between TSA field offices, TSA senior leadership, and DHS. The most significant security breaches and incidents are tracked and reported in real-time for TSA senior leadership and briefed at the Administrator's Daily Intelligence Brief.

- Executive Summary Report—a daily report which includes details on security breaches and incidents that were reported in the previous 24-hour period to the Transportation Security Operations Center. This report is widely distributed and used by managers and senior executives throughout the Agency. The Executive Summary Report is also included in the Administrator's Daily Intelligence Brief.

- TSA's Management Controls Program—this program sets policies, procedures, and the basic structure for TSA's management oversight and accountability program. As part of TSA's Management Controls Program, each hub airport is responsible for completing the FSD Office of Inspection Program/Internal Control Checklist consisting of eight checklists and performing regular internal control assessments throughout the year. TSA's Office of Inspection sends Inspectors to each airport every 4 years to review assessments, supporting materials, and existing processes to ensure that airports are compliant with TSA's policies and directives.

- TSA formed an Assessment Team in March 2010. This team visited 20 airports to focus on proper training and ensuring a common understanding of security breaches. The team reviewed breach containment plans, observed breach drills, shared best practices, and conducted training to increase TSA's proficiency in handling and containing breaches. TSA also compiled a number of resources to assist FSDs with managing and mitigating security breaches, such as guidance on developing Security Breach Plans for their airports, conducting meaningful security breach drills, training programs and training aids for TSA employees, and tools for conducting appropriate after action reviews for significant airport security breaches. Additionally, TSA developed a centralized website which contains all these resources.

**Breach Data Not Consistently Reported, Tracked, and Analyzed**

TSA does not have an effective mechanism in place to gather information about all security breaches and cannot use the information to monitor trends or make general improvements to security. Local TSA airport employees do not always properly report and track all security breaches in PARIS. For each of the six airports we visited, we compared local records of security breaches occurring between January 1, 2010, and May 31, 2011, with information reported in PARIS.

We identified that only [redacted] (42%) of the [redacted] security breaches we reviewed in files were reported in PARIS under any category. For instance, Newark reported only [redacted] security breaches in PARIS between January 1, 2010, and May 31, 2011. However, the number of actual security breach incident report files reviewed at Newark was [redacted]. Figure 3 shows the number of security breaches reported in PARIS compared to the higher number of actual security breaches identified during our incident report review.

**Figure 3: Comparison of Security Breaches Reported in PARIS to Security Breach Incident Report Files, January 1, 2010 to May 31, 2011**

[redacted]
🟦 PARIS Reported Incidents
🟥 Total Number of Incidents OIG Reviewed at Airport

Of the [redacted] incidents reported in PARIS, [redacted] were not properly identified under categories such as sterile area access event, improper/no screening, or security breach. For example, no incident report was filed under the categories of security breach, sterile area access event, and improper/no screening for a loaded firearm entering the sterile area in a carry-on bag. Through a review of disciplinary actions against the TSOs, we discovered that this incident was reported in PARIS under the broad category "actual dangerous/deadly item," not "improper/no screening."

Another example of improper reporting occurred at one airport where TSA did not report an incident when a passenger was allowed to proceed into the sterile area without a valid boarding pass. TSA management at the airport said this incident was not reportable in PARIS based on their interpretation of the guidance. However, TSA headquarters officials informed us that this incident should be reported in PARIS. At another airport, TSA did not report an incident where a bag containing an unknown liquid was improperly cleared and grabbed by the passenger before the screening process was complete.

TSA performs minimal tracking and analysis of security breach data. TSA's Office of Compliance Inspection and Enforcement Analysis is responsible for collecting, tracking, and analyzing PARIS data. According to TSA officials, the agency tracks and analyzes breach data only upon request and produces ad hoc reports. These reports contain information such as the number of security incidents reported by airport, demographic location, or threat type.

Without accurate and complete information and analysis, TSA is limited in its ability to correct and resolve security vulnerabilities. TSA could have a valuable source of security breach data if incidents were consistently reported in PARIS. The data could be used to detect security vulnerabilities and identify trends among airports nationwide.

## **Corrective Actions Were Not Always Taken To Address Breach Vulnerabilities**

At the six airports visited, TSA did not always take action or document their actions to correct security breach vulnerabilities. During our review, we identified documentation of corrective actions for only [redacted] (53%) of the [redacted] breaches we reviewed.

Table 2 shows the number of security breach incident reports reviewed and whether corrective action was taken to prevent or minimize future security breaches.

**Table 2: Number of Security Breaches Reviewed and Corrective or Punitive Actions Taken and Documented**

| Number of Security Breaches (January 1, 2010–May 31, 2011) | | | |
|---|---|---|---|
| **Airport** | **Breaches Reviewed** | **Corrective/ Punitive Action Taken/Documented** | **Percentage** |
| [redacted] | [redacted] | [redacted] | 42% |
| [redacted] | [redacted] | [redacted] | 48% |
| [redacted] | [redacted] | [redacted] | 61% |
| [redacted] | [redacted] | [redacted] | 50% |
| [redacted] | [redacted] | [redacted] | 88% |
| [redacted] | [redacted] | [redacted] | 57% |
| **Total** | [redacted] | [redacted] | **53%** |

Corrective and punitive actions included training; letters of counseling; reprimand; suspension; administrative inquiries; changes to checkpoint configuration; and enforcement actions issued against passengers, airline, or airport employees. For instance, TSA can provide remedial training to TSOs for knowledge gaps or deficits and initiate civil and criminal procedures against passengers, airlines, and airport employees for violating TSA regulations. Additionally, TSA may adjust the design, layout, infrastructure, or staffing associated with screening checkpoints to mitigate vulnerabilities.

## Guidance for Reporting Breaches Was Unclear

TSA's current operations directives for security breach definitions and reporting requirements are unclear and contribute to reporting inconsistencies, which hinders TSA's ability to track and analyze breach trends across airports. Under the PARIS reporting system, a security incident could fall under more than one of 33 categories in PARIS because of the ambiguity of the operations directive as currently written. For example,

- TSA at one airport reported an improper bag handoff incident in PARIS as a sterile area access event. However, TSA at another airport reported four similar incidents as security breaches.

- We identified two similar security breaches reported at different airports involving a knife that went undetected through screening and into the sterile area. In PARIS, one airport noted the breach as an improper/no screening event while another airport reported the breach as a sterile area access event.

- TSA at one airport did not report a passenger who entered the sterile area with a handwritten boarding pass because management did not think the scenario fell under any PARIS or TSOC requirements. In contrast, two other airports reported this type of incident in PARIS.

TSA's Operations Directive OD-400-50-5-3, *Management of Security Breaches*, contains a different definition of what constitutes a breach of security than that found in the operations directive for PARIS reporting. For example, Operations Directive 400-50—5-3 indicates the following:

- A security breach is defined as "any incident involving unauthorized and uncontrolled access by an individual or prohibited item into a sterile area or secured area of an airport that is determined by TSA to present an immediate and significant risk to life, safety, or the security of the transportation network [redacted]"
- Access events that do not specifically meet the criteria of a security breach are considered security incidents/events and should not necessitate the closure of any portion of the airport.

In TSA's Operations Directive 400-18-1, *Reporting Security Incidents via PARIS*, the term "security breach" is defined as follows:

> "Incidents involving an individual gaining access to the sterile area at the screening checkpoint or a collocated operational exit lane without submitting to all screening and inspections of his/her person and accessible property in accordance with procedures contained in the Screening Checkpoint Standard Operating Procedures."

TSA headquarters could have a valuable source of breach data in the PARIS system if consistently reported by TSA at the airports. PARIS could provide data identifying not only the raw number of incidents taking place at the Nation's airports but also why they occurred. Vulnerabilities detected at one airport or in one region could be identified and communicated to every FSD in the country so that lessons learned at one location could be applied nationwide.

## Oversight for Reporting and Tracking Breaches Was Limited

TSA does not provide the necessary oversight to ensure accurate and complete reporting, tracking, and correcting of security breaches. TSA could not provide evidence that it reviews or validates data submitted by airports in PARIS and the TSOC for accuracy, omissions, or errors. TSA does not have a process to ensure that all security breaches are identified and reported. It does not review security breaches to identify discrepancies with the categories used by different airports when reporting events, such as those found during our review.

FSDs are responsible for reporting all security incidents that occur at their airport to PARIS and TSOC. TSA coordination center managers at the airports are responsible for reviewing and validating the data submitted into PARIS and TSOC. However, based on our review of incident files and security breaches reported in PARIS, TSA is not reviewing and reconciling the data submitted in PARIS.

At one airport we visited, local TSA management was unaware that it was not reporting all incidents in PARIS. Without any review or oversight of what the airport reported, this gap in reporting was not apparent until our review.

## Conclusion

Without an effective mechanism in place to gather information about all security breaches, TSA is unable to monitor trends or make general improvements to security. Airports need a clear definition and guidance for identifying and reporting security breaches through PARIS so TSA can capture an accurate understanding of security breaches occurring at airports nationwide.

Without an effective oversight program to ensure security breach data is reported, tracked, analyzed, and corrective actions are taken, TSA is limiting its ability to prevent, minimize, respond to, and take corrective actions against security breaches in the future. Consequently, the agency misses opportunities to identify and correct vulnerabilities to strengthen aviation security.

## Recommendations

We recommend that the Transportation Security Administration Assistant Administrator, Office of Security Operations:

**Recommendation #1:** Refine and use one comprehensive definition of what constitutes a security breach that can be universally reported to Performance and Results Information System and the Transportation Security Operations Center. Once issued, ensure that this guidance is used and clearly understood throughout the agency.

**Recommendation #2:** Develop a comprehensive oversight program to ensure:

a. That security breaches are accurately reported based on the revised definition, and the events are properly tracked and analyzed for trends. This should include local and national reporting that can be validated at the headquarters level.
b. The agency consistently takes actions to correct vulnerabilities resulting from security breaches.

## Management Comments and OIG Analysis

TSA provided comments to the draft report. A copy of the response in its entirety is included in appendix B. TSA agreed with the recommendations in the report and identified planned actions to address the recommendations made within the report. Both recommendations are unresolved and remain open. TSA also provided technical comments and suggested revisions to sections of the report. When appropriate, we made changes to reflect the suggested revisions.

**Management Comments to Recommendation 1**

**TSA concurs.** The Administrator agreed that a single definition of Security Breach should exist in all relevant policy documents. TSA is coordinating appropriate revisions to the relevant Operations Directives.

**OIG Analysis**: TSA's planned actions sufficiently address the recommendation. The recommendation is unresolved and will remain open until TSA provides copies of the revised Operations Directives.

**Management Comments to Recommendation 2**

**TSA concurs.** The Administrator responded that TSA is working to enhance its oversight of airport security breaches and will better leverage PARIS to more accurately report, track and analyze trends. TSA is also updating its airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels. This will allow TSA Regional Directors and headquarters leadership to better assess airport performance and correct vulnerabilities.

**OIG Analysis:** TSA's planned actions sufficiently address the recommendation. The recommendation is unresolved and will remain open until TSA provides documentation to support the actions taken.

We conducted this audit in response to a request from Senator Lautenberg of the Senate Appropriations Committee. The letter is included as appendix C. The Senator was concerned about a series of security incidents reported at Newark Liberty International Airport. In addition to addressing Senator Lautenberg's specific concerns, we also determined whether TSA has an effective mechanism to use the information gathered from individual airports to identify measures that could be used to improve security nationwide.

We interviewed officials and personnel from various offices and groups within TSA involved in security operations, including the Office of Security Operations, Compliance, and Field Operations Divisions; Office of Technical Training; Office of Improvement Branch; and Transportation Security Operations Center. We reviewed PARIS reports from January 2008 through May 2011, as well as TSOC reports from the selected airports. Through an analysis of the security incident reports and PARIS documentation, we identified differences in PARIS reporting among airports.

Interviews and supporting documents provided a detailed understanding of TSA's policies and procedures for reporting security incidents at airports. They also provided insight into how TSA uses this data to detect security vulnerabilities and to prevent breaches from occurring.

To determine the incident reporting standards mandated by TSA, we examined the following TSA operating directives:

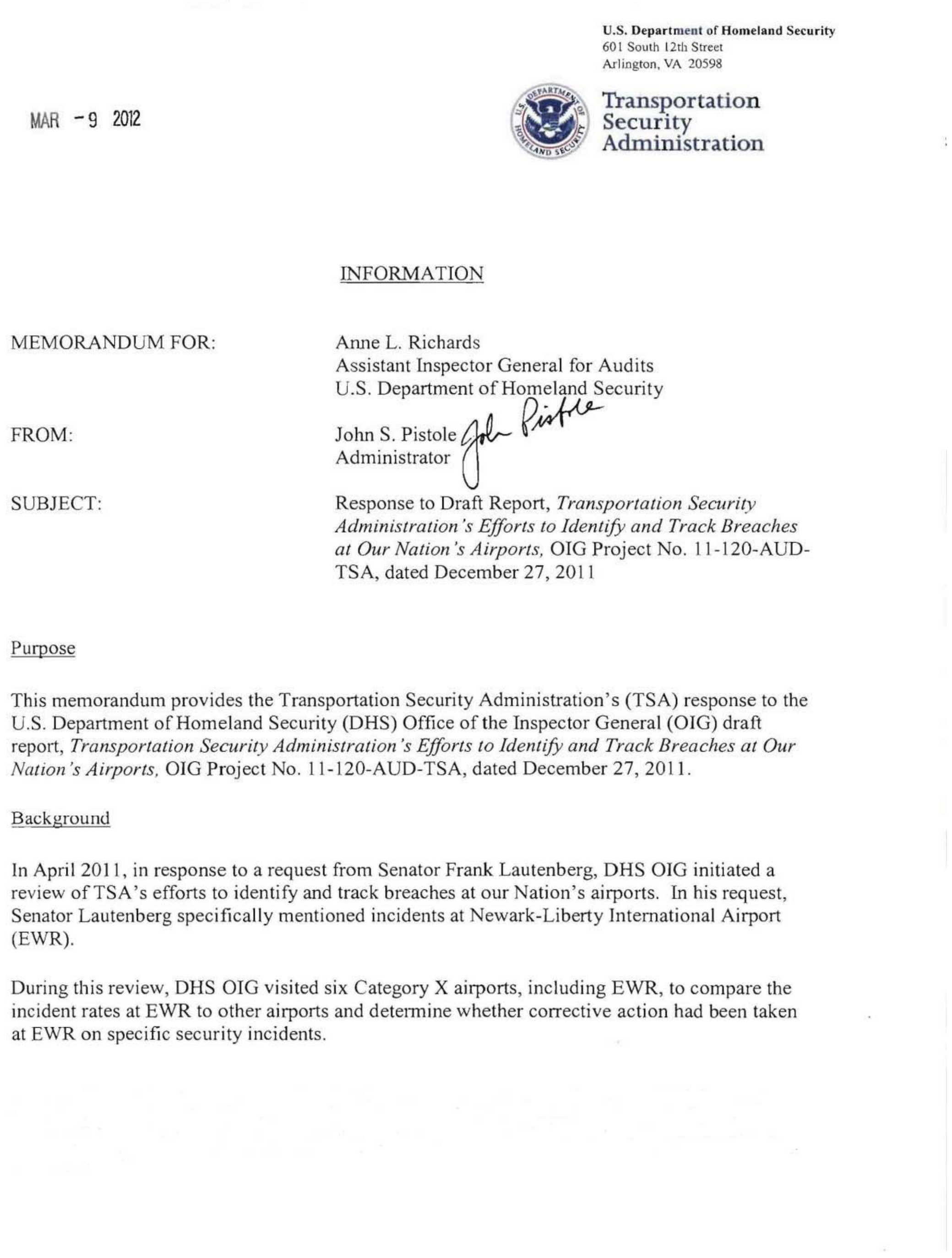
- OD-400-18-1: *Reporting Security Incidents via PARIS*
- OD-400-18-2D: *Reporting Security Incidents to the Transportation Security Operations Center*
- OD-400-50-5-3: *Management of Security Breaches*

We selected six airports to review, including Newark Liberty International Airport, [redacted]. The three remaining airports were selected based on the airport screening performance, passenger volume, number of TSA employees, history of airport management based on TSA headquarter interviews, and regional variation. These airports were [redacted]. All the airports we visited are within the top 20 Category X airports in passenger volume. The method of selecting our locations prevents us from projecting the findings on a national level.

At each airport, we interviewed TSA management to discuss airport security operations and reviewed security breach plans. We also met with representatives of other key stakeholders to obtain an understanding of their role as it relates to security. These included the airport authority, local police, and major air carriers operating from that airport. We reviewed [redacted] security incident reports of security breaches documented by the airports that occurred between January 2010 and May 2011. We looked only at those that fell under the categories of security breaches, improper/no screening, and sterile area security events. These incident reports were provided by TSA management at each location and contained information on security events that are reportable to PARIS and TSOC.

We conducted this performance audit between April and September 2011 pursuant to the *Inspector General Act of 1978*, as amended, and 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

## Appendix B
## Management Comments to the Draft Report



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

Transportation
Security
Administration

MAR -9 2012

INFORMATION

MEMORANDUM FOR: Anne L. Richards
Assistant Inspector General for Audits
U.S. Department of Homeland Security

FROM: John S. Pistole
Administrator

SUBJECT: Response to Draft Report, *Transportation Security Administration's Efforts to Identify and Track Breaches at Our Nation's Airports,* OIG Project No. 11-120-AUD-TSA, dated December 27, 2011

Purpose

This memorandum provides the Transportation Security Administration's (TSA) response to the U.S. Department of Homeland Security (DHS) Office of the Inspector General (OIG) draft report, *Transportation Security Administration's Efforts to Identify and Track Breaches at Our Nation's Airports,* OIG Project No. 11-120-AUD-TSA, dated December 27, 2011.

Background

In April 2011, in response to a request from Senator Frank Lautenberg, DHS OIG initiated a review of TSA's efforts to identify and track breaches at our Nation's airports. In his request, Senator Lautenberg specifically mentioned incidents at Newark-Liberty International Airport (EWR).

During this review, DHS OIG visited six Category X airports, including EWR, to compare the incident rates at EWR to other airports and determine whether corrective action had been taken at EWR on specific security incidents.

DHS OIG's report concludes that:

1.) Although TSA has several programs and initiatives in place that report and track identified security breaches, TSA does not have a comprehensive oversight program to gather information about all security breaches and therefore cannot use the information to monitor trends or make general improvements to security.

2.) TSA does not provide the necessary guidance and oversight to ensure that all breaches are consistently reported, tracked, and corrected.

At the conclusion of the report, DHS OIG provides two recommendations for TSA to address.

Discussion

TSA understands that risk cannot be completely eliminated; instead, we focus our efforts on risk mitigation. The best defense against threats to our transportation systems remains a risk-based, intelligence-driven, layered security approach that employs a range of measures, both seen and unseen. Each security layer TSA employs is capable of stopping a terrorist attack, and in combination, their security value is multiplied, creating a much stronger and formidable system. A terrorist who has to overcome multiple security layers to carry out an attack is more likely to be preempted, deterred, or to fail during the attempt.

Detecting, responding to, and mitigating the risks associated with security breaches and incidents comprise a critical aspect of TSA's security model. Early identification, containment, and resolution of breaches through the execution and coordination of defined processes and procedures with all airport stakeholders are essential.

TSA appreciates DHS OIG's work to identify opportunities to further develop and improve TSA's ability to mitigate security breaches at our Nation's airports. TSA values OIG's recognition of the work TSA has done since 2010 to improve airport's proficiency in managing and containing airport security breaches by sharing best practices, ensuring TSA staff receive proper training, maintaining up to date breach containment plans, and regularly conducting security breach drills. TSA also appreciates DHS OIG's recognition of the steps taken at EWR to improve operations and address checkpoint vulnerabilities, including the "Back to Basics" campaign and the *Newark Commitment to Excellence*. The current EWR Federal Security Director (FSD) and Deputy FSD have been in place since April 24, 2011, and July 31, 2011, respectively; and both have made significant changes in procedures, processes, and workforce communication that have made a positive difference in the workforce climate and security posture of the airport.

As DHS OIG points out, TSA has several programs and initiatives for reporting and tracking airport security breaches. Each year, TSA collects thousands of records of incidents and security breaches occurring at airports and at other transportation facilities. These airport security breach and incident reports are widely disseminated to appropriate TSA program offices through various

[redacted]

channels of reporting. TSA leadership regularly reviews reports on significant airport security breaches and incidents, including a daily briefing provided as part of the Administrator's Daily Intelligence Brief. TSA acknowledges that it can further develop and expand its oversight programs for gathering and tracking airport security breaches.

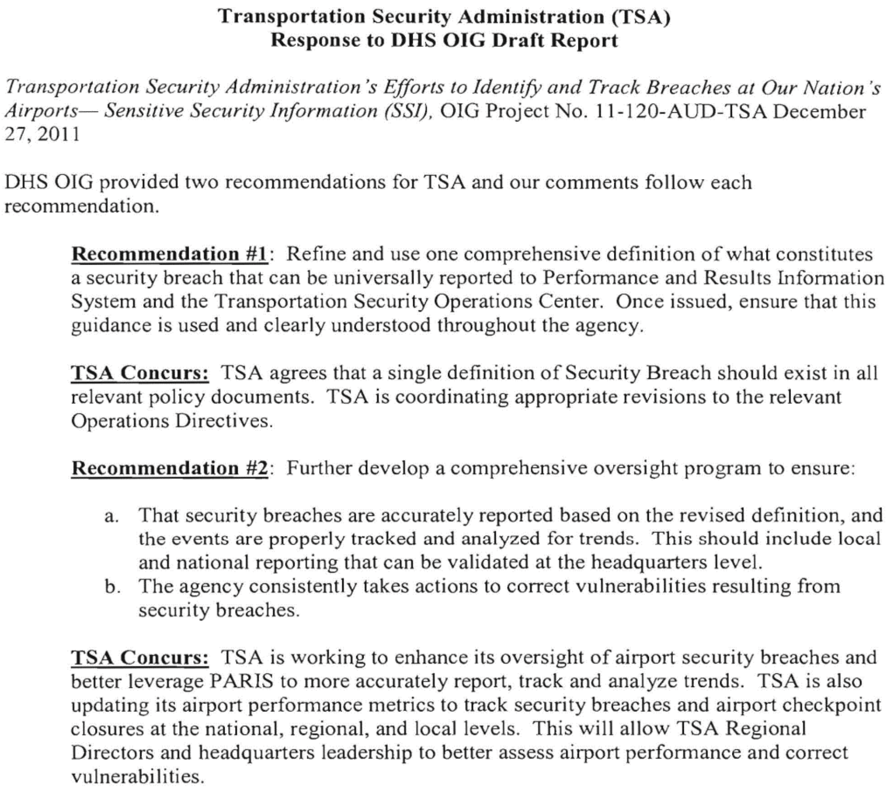
TSA also acknowledges that there is opportunity to improve its data collection and analysis of airport security breaches. TSA currently publishes a wide variety of reports and analyses of security breaches based on incident reports filed in the Performance and Results Information System (PARIS). PARIS is the focal point for reporting information concerning security breaches and related activity, with an emphasis on security breaches that result in civil enforcement investigations. Since 2004, this information technology application has provided users across the Agency with a custom-view "Dashboard" that provides a running total and description of security incidents as they are submitted into the database by each airport. Moreover, the PARIS Security Reports Module provides an end-user with a broader capability to view incident reports based on a wide variety of parameters (e.g., date range, location, type of incident, and more). PARIS reports can be generated for various categories of airport security incidents and can be organized by: frequency of reporting; airport or incident type; airport category, date, and time; and various other parameters. TSA acknowledges that it can better leverage PARIS to more accurately track and analyze security breach data to identify trends and develop appropriate mitigation strategies.

TSA is enhancing its performance management and oversight of FSDs and TSA field operations through its new Regional Director (RD) structure. Improvements will include the use of specific performance metrics designed to give RDs and TSA headquarters leadership an overview of each region's overall performance and organizational health. At a minimum, the primary performance metrics will be reviewed and analyzed by TSA senior leadership during monthly RD meetings. One of the updated performance metrics that TSA is finalizing is the Incident Management Indicator (IMI), which will track the number of security breaches and airport checkpoint closures throughout each region. The IMI will also incorporate new data entry requirements for security breaches, checkpoint closures, incident management training, security breach drills, and tabletop exercises conducted with airport stakeholders.

Conclusion

TSA appreciates the opportunity to provide feedback to DHS OIG on its draft findings and recommendations.

## Appendix B
## Management Comments to the Draft Report



**Transportation Security Administration (TSA)**
**Response to DHS OIG Draft Report**

*Transportation Security Administration's Efforts to Identify and Track Breaches at Our Nation's Airports— Sensitive Security Information (SSI),* OIG Project No. 11-120-AUD-TSA December 27, 2011

DHS OIG provided two recommendations for TSA and our comments follow each recommendation.

**Recommendation #1**: Refine and use one comprehensive definition of what constitutes a security breach that can be universally reported to Performance and Results Information System and the Transportation Security Operations Center. Once issued, ensure that this guidance is used and clearly understood throughout the agency.

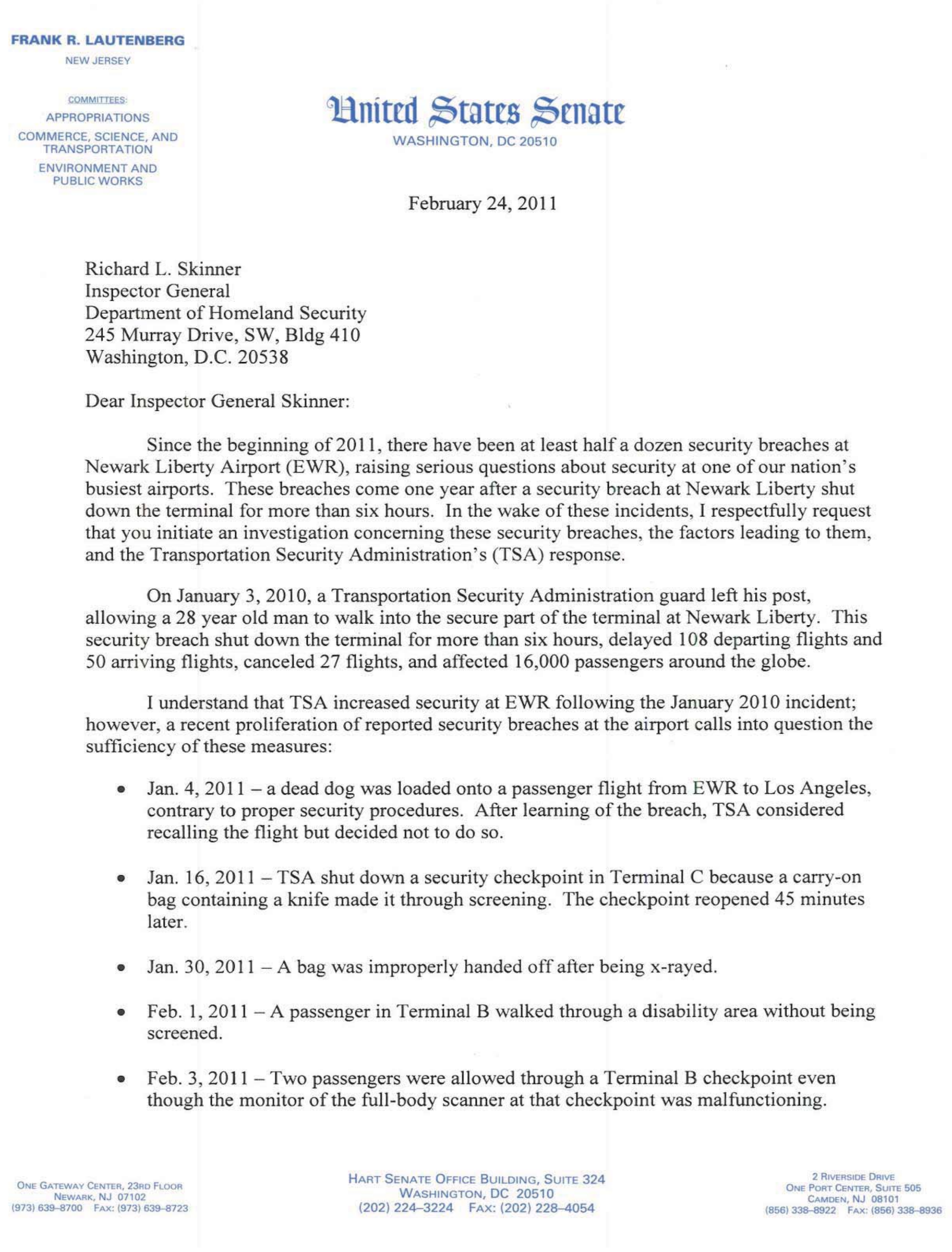
**TSA Concurs:** TSA agrees that a single definition of Security Breach should exist in all relevant policy documents. TSA is coordinating appropriate revisions to the relevant Operations Directives.

**Recommendation #2**: Further develop a comprehensive oversight program to ensure:

a. That security breaches are accurately reported based on the revised definition, and the events are properly tracked and analyzed for trends. This should include local and national reporting that can be validated at the headquarters level.
b. The agency consistently takes actions to correct vulnerabilities resulting from security breaches.

**TSA Concurs:** TSA is working to enhance its oversight of airport security breaches and better leverage PARIS to more accurately report, track and analyze trends. TSA is also updating its airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels. This will allow TSA Regional Directors and headquarters leadership to better assess airport performance and correct vulnerabilities.

# Appendix C
# Senator Lautenberg Request Letter



FRANK R. LAUTENBERG
NEW JERSEY

COMMITTEES:
APPROPRIATIONS
COMMERCE, SCIENCE, AND TRANSPORTATION
ENVIRONMENT AND PUBLIC WORKS

United States Senate
WASHINGTON, DC 20510

February 24, 2011

Richard L. Skinner
Inspector General
Department of Homeland Security
245 Murray Drive, SW, Bldg 410
Washington, D.C. 20538

Dear Inspector General Skinner:

Since the beginning of 2011, there have been at least half a dozen security breaches at Newark Liberty Airport (EWR), raising serious questions about security at one of our nation's busiest airports. These breaches come one year after a security breach at Newark Liberty shut down the terminal for more than six hours. In the wake of these incidents, I respectfully request that you initiate an investigation concerning these security breaches, the factors leading to them, and the Transportation Security Administration's (TSA) response.

On January 3, 2010, a Transportation Security Administration guard left his post, allowing a 28 year old man to walk into the secure part of the terminal at Newark Liberty. This security breach shut down the terminal for more than six hours, delayed 108 departing flights and 50 arriving flights, canceled 27 flights, and affected 16,000 passengers around the globe.

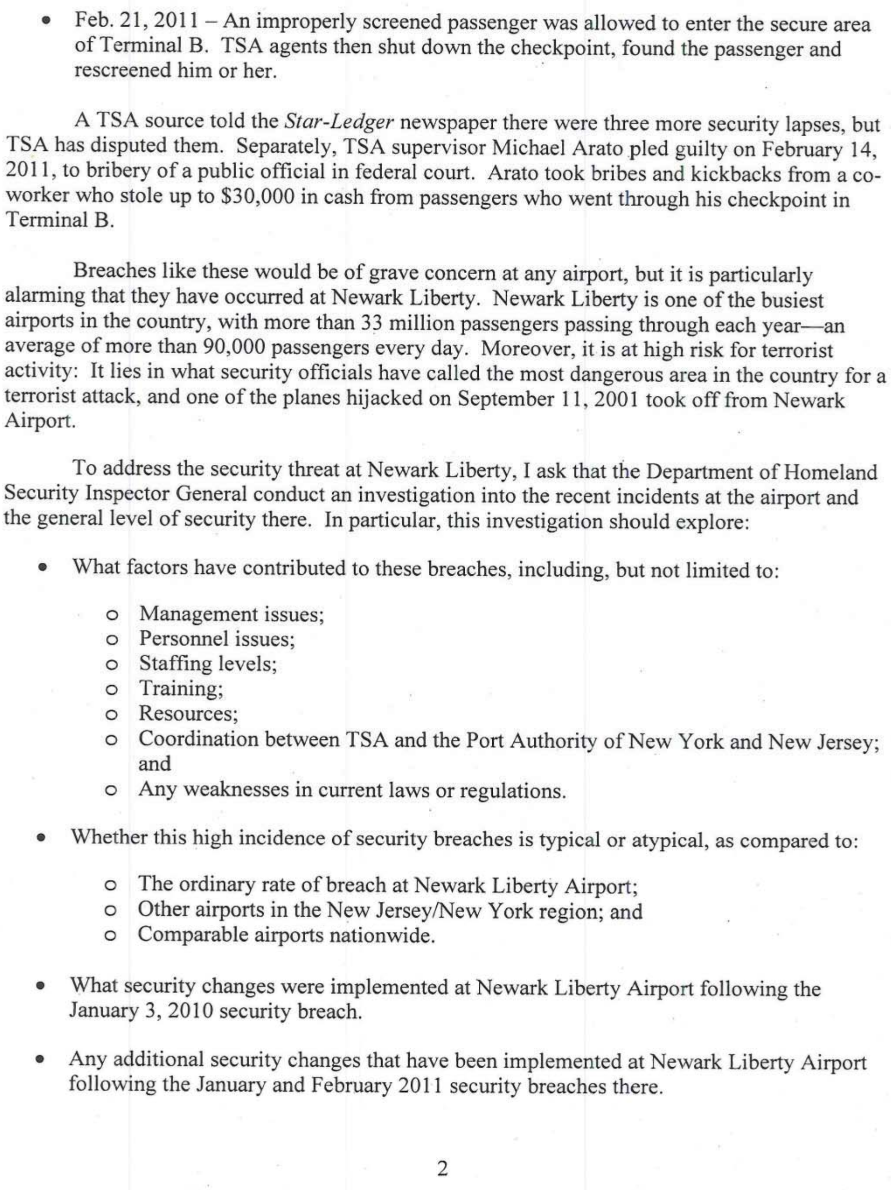
I understand that TSA increased security at EWR following the January 2010 incident; however, a recent proliferation of reported security breaches at the airport calls into question the sufficiency of these measures:

- Jan. 4, 2011 – a dead dog was loaded onto a passenger flight from EWR to Los Angeles, contrary to proper security procedures. After learning of the breach, TSA considered recalling the flight but decided not to do so.
- Jan. 16, 2011 – TSA shut down a security checkpoint in Terminal C because a carry-on bag containing a knife made it through screening. The checkpoint reopened 45 minutes later.
- Jan. 30, 2011 – A bag was improperly handed off after being x-rayed.
- Feb. 1, 2011 – A passenger in Terminal B walked through a disability area without being screened.
- Feb. 3, 2011 – Two passengers were allowed through a Terminal B checkpoint even though the monitor of the full-body scanner at that checkpoint was malfunctioning.

ONE GATEWAY CENTER, 23RD FLOOR
NEWARK, NJ 07102
(973) 639–8700 FAX: (973) 639–8723

HART SENATE OFFICE BUILDING, SUITE 324
WASHINGTON, DC 20510
(202) 224–3224 FAX: (202) 228–4054

2 RIVERSIDE DRIVE
ONE PORT CENTER, SUITE 505
CAMDEN, NJ 08101
(856) 338–8922 FAX: (856) 338–8936



- Feb. 21, 2011 – An improperly screened passenger was allowed to enter the secure area of Terminal B. TSA agents then shut down the checkpoint, found the passenger and rescreened him or her.

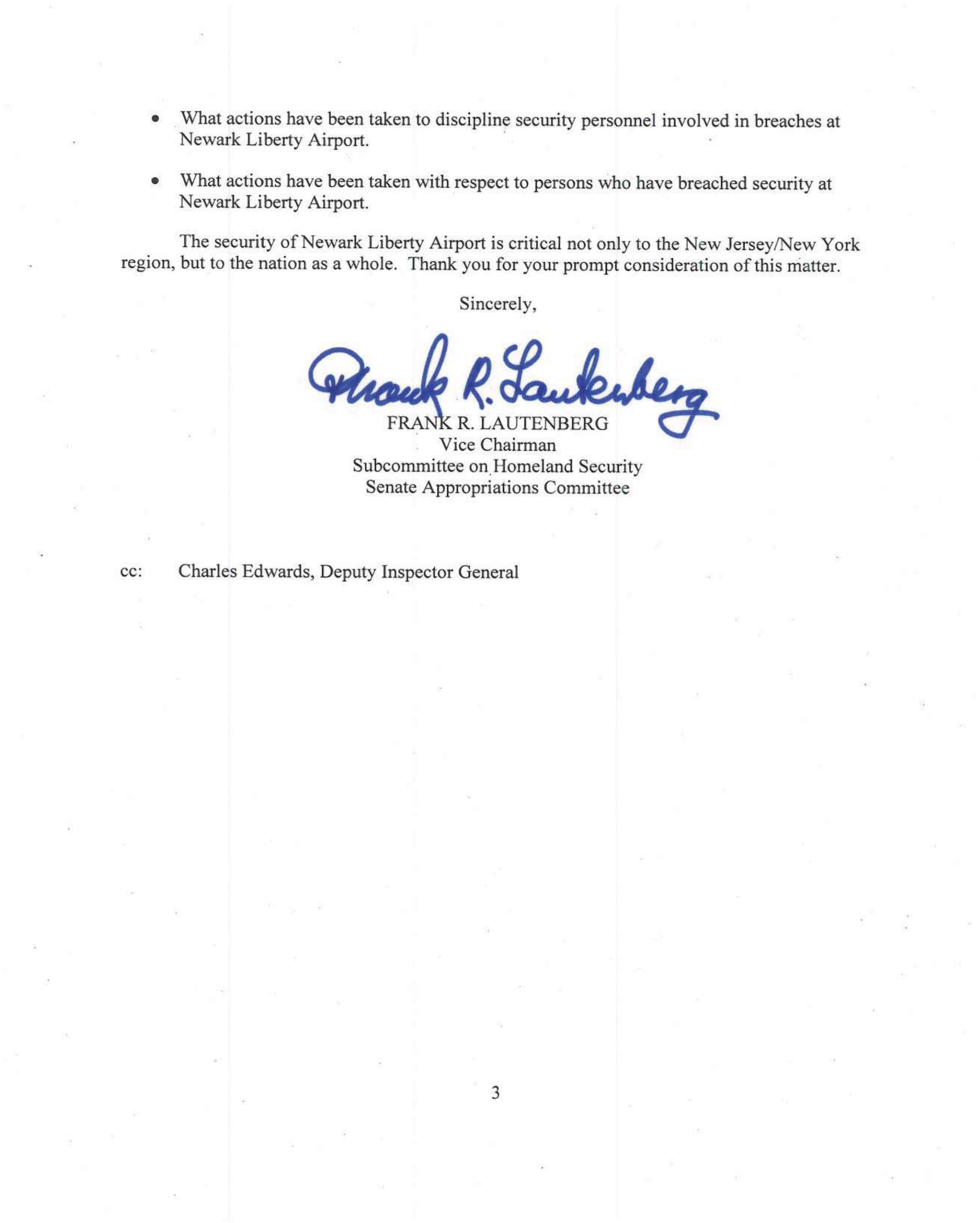
A TSA source told the *Star-Ledger* newspaper there were three more security lapses, but TSA has disputed them. Separately, TSA supervisor Michael Arato pled guilty on February 14, 2011, to bribery of a public official in federal court. Arato took bribes and kickbacks from a co-worker who stole up to $30,000 in cash from passengers who went through his checkpoint in Terminal B.

Breaches like these would be of grave concern at any airport, but it is particularly alarming that they have occurred at Newark Liberty. Newark Liberty is one of the busiest airports in the country, with more than 33 million passengers passing through each year—an average of more than 90,000 passengers every day. Moreover, it is at high risk for terrorist activity: It lies in what security officials have called the most dangerous area in the country for a terrorist attack, and one of the planes hijacked on September 11, 2001 took off from Newark Airport.

To address the security threat at Newark Liberty, I ask that the Department of Homeland Security Inspector General conduct an investigation into the recent incidents at the airport and the general level of security there. In particular, this investigation should explore:

- What factors have contributed to these breaches, including, but not limited to:
    - Management issues;
    - Personnel issues;
    - Staffing levels;
    - Training;
    - Resources;
    - Coordination between TSA and the Port Authority of New York and New Jersey; and
    - Any weaknesses in current laws or regulations.
- Whether this high incidence of security breaches is typical or atypical, as compared to:
    - The ordinary rate of breach at Newark Liberty Airport;
    - Other airports in the New Jersey/New York region; and
    - Comparable airports nationwide.
- What security changes were implemented at Newark Liberty Airport following the January 3, 2010 security breach.
- Any additional security changes that have been implemented at Newark Liberty Airport following the January and February 2011 security breaches there.

## Appendix C
## Senator Lautenberg Request Letter



- What actions have been taken to discipline security personnel involved in breaches at Newark Liberty Airport.

- What actions have been taken with respect to persons who have breached security at Newark Liberty Airport.

The security of Newark Liberty Airport is critical not only to the New Jersey/New York region, but to the nation as a whole. Thank you for your prompt consideration of this matter.

Sincerely,

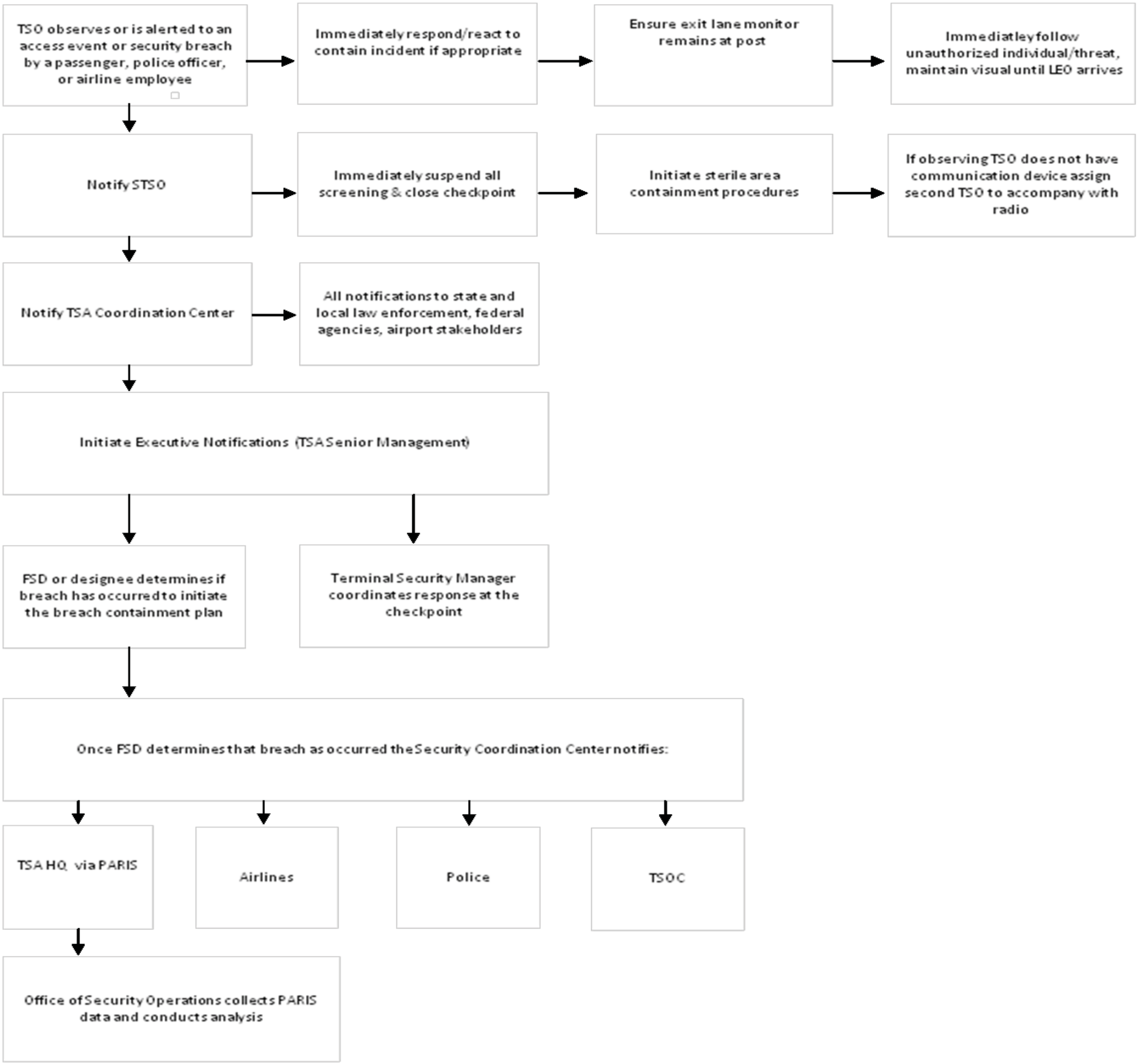
Frank R. Lautenberg

FRANK R. LAUTENBERG
Vice Chairman
Subcommittee on Homeland Security
Senate Appropriations Committee

cc: Charles Edwards, Deputy Inspector General

## Appendix D
## Process for Identifying, Reporting and Tracking Security Breaches

Due to the static presentation of the flowchart below, the process does not reflect the fluid steps occurring simultaneously to respond to a security incident. TSA leadership, law enforcement, and other stakeholders may be brought in earlier than is depicted in the flowchart, to mitigate an incident.


TSO observes or is alerted to an access event or security breach by a passenger, police officer, or airline employee
Immediately respond/react to contain incident if appropriate
Ensure exit lane monitor remains at post
Immediatley follow unauthorized individual/threat, maintain visual until LEO arrives
Notify STSO
Immediately suspend all screening & close checkpoint
Initiate sterile area containment procedures
If observing TSO does not have communication device assign second TSO to accompany with radio
Notify TSA Coordination Center
All notifications to state and local law enforcement, federal agencies, airport stakeholders
Initiate Executive Notifications (TSA Senior Management)
FSD or designee determines if breach has occurred to initiate the breach containment plan
Terminal Security Manager coordinates response at the checkpoint
Once FSD determines that breach as occurred the Security Coordination Center notifies:
TSA HQ via PARIS
Airlines
Police
TSOC
Office of Security Operations collects PARIS data and conducts analysis

Source: DHS OIG

## Appendix E
## Security Breach Controls and Promising Practices

During our visits to six airports, we determined TSA has initiated a number of controls and promising practices. The following list is not exhaustive but represents a few examples of the controls and practices at each airport.

| |
|---|
| |
| • Exit Lanes: TSA installed motion sensors at exit lanes to detect when people are walking the wrong way.<br>• Breach Drills: As part of the breach containment plan, breach drills are conducted to reinforce actions to be taken when responding to an actual security breach.<br>• After-Action Reports: TSA prepares after-action reports that summarize details of security breaches, including the causes and corrective actions. |
| [redacted] |
| • Crossings Pilot Program: This TSA headquarters-vetted pilot program uses scenarios to test the individual performance of a TSO and the actions that he or she takes during the scenario. The program reviews the tasks and responsibilities of the TSOs involved with the screening security operations at the airport. Transportation Security Specialists for Explosives and other TSA employees develop and carry out scenarios to view how TSOs respond to each scenario tested at the checkpoint or checked baggage area. Rather than focus on placing individual blame, the Crossings Program concentrates on locating systemic weaknesses.<br>• Aviation Screening Assessment Program and Covert Testing: TSA management uses these programs to spot vulnerabilities at the checkpoints, such as the checkpoint layout and TSOs' performance. They can also use the Aviation Screening Assessment Program results to determine what improvements can be made to security operations at the airport.<br>• Management Oversight: Transportation Security Inspectors and Transportation Security Managers observe TSOs at the checkpoints and checked baggage areas to spot vulnerabilities with their performance. |
| [redacted] |
| • Quality Assurance Team: To ensure compliance with SOP, a team composed of a manager, supervisors, and senior screeners regularly tour the airport to observe and review the performance of checkpoint staff. Observations are made covertly both to assess compliance and to continually reinforce best practices.<br>• X Ray Machines: Plans are underway to enhance the technology infrastructure available to screeners. New x ray machines will have dual screens to show two angles on bags being scanned, [redacted]<br>• Facility Service Unit: This unit is composed of TSA employees who tour the airport, identify problems, and where possible make improvements relating to checkpoint designs, including closed-circuit television installations. They work with airport stakeholders[redacted] [redacted] [redacted]and air carriers to improve the checkpoint layouts and ensure that new checkpoint configurations comply with all TSA requirements. |
| [redacted] |
| • Daily Stakeholders Briefing: An airport stakeholders briefing is held daily. Stakeholders comprise approximately 70 individuals from TSA [redacted], Customs and Border Protection, Joint Terrorism Task Force, Airport Fire and Rescue, security contractors, and major airlines. Stakeholders report information affecting airport operations. The |

briefing fosters open communication and relationship building between the stakeholders and TSA.

- Exit Lanes: Frosted doors at the exit lanes prevent people on the non-sterile side from seeing through the doors to passengers exiting the sterile area.
- New Technology: [redacted] developed a prototype of an advanced decision support module. The technology is an all-in-one handheld device enabling parties to be connected through a smart phone. This module can help TSA and other federal agencies assess and mitigate security incidents. It provides accurate and timely information during a telephone bridge call, image review in real time of the security event, and notifications of what is happening with the event and in other parts of the airport.

[redacted]

- Terminal Chokepoints: The chokepoints restrict access to other sections of the main terminal during a security breach, which isolates the threat item or suspected individual to one area.
- TSA Employee Training: TSA management is providing more classroom and floor training to supervisors and managers. Additionally, TSA coordinates with other entities to deliver training to TSA employees. For example, Customs and Border Protection provided fraudulent document training to the TSOs assigned as travel document checkers at the airport.
- Airport Police Training: TSA trained all police officers within the [redacted] Airport Police Division on TSA policies, procedures, and protocols during a security breach. During training, TSA provides an overview of TSA employees' responsibilities and duties so that police officers understand everyone's role in airport security. TSA also offered training to the police officers on the new advanced technology screening equipment so the Airport Police understand new procedures concerning these machines. The training and information sessions are important in maintaining good relationships between TSA and the Airport Police.

[redacted]

- Terminal Chokepoints: Chokepoints throughout the airport restrict access to the entire terminal during a security breach.
- Guidance and Training: Due to the number of security breaches resulting from [redacted] between TSOs and the inability to secure bags at the checkpoint for secondary screening, TSA issued guidance through memorandums and offered additional training to the TSO workforce to improve their performance and ensure compliance with these checkpoint screening procedures.
- Breach Response Protocols: [redacted] has a security breach containment plan with procedures and processes that TSA will implement during a security breach. In addition to a designated code phrase used by TSA staff to initiate breach protocols, the airport has a breach alarm button. This alarm button activates an amber light system in the main terminal, supervisory TSO offices, and the airport's Coordination Center. The amber light system notifies the [redacted] Police Department to dispatch officers to respond to a security breach. The system also notifies air carrier gate agents to stop all aircraft boarding and deplaning activities.

## Appendix F
## PARIS Categories

| PERFORMANCE AND RESULTS INFORMATION SYSTEM (PARIS)<br>REPORTING CATEGORIES | |
|---|---|
| 1. | Access Control |
| 2. | Actual Deadly/Dangerous Item |
| 3. | Air Piracy |
| 4. | Aircraft Accident |
| 5. | Bomb Threat |
| 6. | Bombing |
| 7. | Chemical/Biological/Radiological Agent Threat |
| 8. | Chemical/Biological/Radiological Incident |
| 9. | Damage to TSA Facilities |
| 10. | Dangerous Goods Incident |
| 11. | Disruptive Airport or Air Carrier Employee |
| 12. | Disruptive Crew Member |
| 13. | Hijacking |
| 14. | Improper/No Screening |
| 15. | Inappropriate Communications/Contact |
| 16. | Natural Disaster |
| 17. | No-Fly List Match |
| 18. | Other |
| 19. | Perimeter Breach |
| 20. | Perimeter Event |
| 21. | Phantom Controller |
| 22. | Sabotage to Aircraft |
| 23. | Security Breach |
| 24. | Selectee List Match |
| 25. | Small Arms Fire (includes chemical agents) |
| 26. | Sterile Area Access Event |
| 27. | Suspected Deadly/Dangerous Item |
| 28. | Suspicious Aircraft |
| 29. | Suspicious Individual |
| 30. | Technological/Mechanical Problems |
| 31. | Threats of Air Piracy |
| 32. | Unattended Baggage |
| 33. | Unruly Passenger |

# Appendix G
# Major Contributors to this Report

Patrick O'Malley, Director
Cheryl Jones, Audit Manager
Kristine Odiña, Analyst in Charge
Philip Emswiler, Program Analyst
Tia Jackson, Program Analyst
Megan McNulty, Program Analyst
Terrell Tindull, Referencer

## Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
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

## Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

## Transportation Security Administration

Administrator
Assistant Administrator, Office of Security Operations
Assistant Administrator, Operational Process and Technology
Transportation Security Administration Audit Liaison

## 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)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

## OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to Department of Homeland Security programs and 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; or

- Write to us at:

  DHS Office of Inspector General/MAIL STOP 2600,<br>
  Attention: Office of Investigation - Hotline,<br>
  245 Murray Drive SW, Building 410<br>
  Washington, DC 20528

The OIG seeks to protect the identity of each writer and caller.