STATEMENT OF CHARLES K. EDWARDS

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

"Access Control Breaches at Our Nation's Airports: Anomalies or Systemic Failures"

May 16, 2012

Good morning Chairman Rogers, Ranking Member Jackson Lee, and Members of the Subcommittee:

I am Charles Edwards, Acting Inspector General for the Department of Homeland Security (DHS) Office of Inspector General (OIG). Thank you for inviting me to testify today about the results of our audits regarding the Transportation Security Administration's (TSA) access controls at our Nation's airports. Since the events of September 11, 2001, TSA has spent billions of dollars on multiple layers of aviation security and relies on those layers of security to ensure the safety of the traveling public.

My testimony today will present the results of three recent audits of aspects of TSA's oversight of security at our nation's airports.[1] Specifically, I will address TSA's oversight of the process to vet airport, or airport vendor, employees prior to giving them badges that allow unescorted access to secure areas; TSA's oversight of airports' physical access controls; and lastly, I will summarize our evaluation of TSA's collection of security breach information which should be used to identify and correct potential vulnerabilities.

Airport Badging Process[2]

We evaluated TSA's oversight of the process for issuing airport security badges. These badges allow an individual unescorted access to secure airport areas, including:

- Sterile Area – A portion of an airport, defined in the airport security program, that provides passengers access to boarding aircraft, and to which the access is generally controlled by TSA through the screening of persons and property.
- Air Operations Area (AOA) – A portion of an airport that includes aircraft movement areas, loading ramps, and safety areas for use by aircraft.
- Security Identification Display Area (SIDA) – A part of the AOA regularly used to load cargo on, or unload cargo from an aircraft. TSA can designate all or portions of the AOA as SIDA.

As of the time of our audit fieldwork, there were approximately 890,000 individuals with 1.2 million active badges that had access to secure areas of airports.[3]

Applicants for these badges are required to undergo a fingerprint-based criminal history records check and have an approved security threat assessment (STA) from TSA before receiving a

[1] The information provided in this testimony is contained in the following reports: *TSA's Oversight of the Airport Badging Process Needs Improvement* (OIG-11-95); *Covert Testing of Access Controls to Secured Airport Areas* (OIG-12-26); and *Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports* (OIG-12-80).

[2] *TSA's Oversight of the Airport Badging Process Needs Improvement* (OIG-11-95)

[3] Employees could have more than one badge if working for multiple employers at the airport or if working at multiple airports.

badge and obtaining unescorted access to secure airport areas. The STA is accomplished by comparing an applicant's information against critical data sets to discern whether the applicant is a threat to transportation or national security.

TSA relies on designated airport operator employees as trusted agents to perform the essential functions of the badging process. Their duties consist of collecting, verifying, and inputting applicant data used for the STA process and fingerprinting applicants for the Criminal History Records Check. Airport operator employees are responsible for ensuring that the badge application is complete with the required biographical and fingerprint data for the STA. Critical data processed from the application includes full legal name, date of birth, place of birth, passport number, and alien registration number. Airports are responsible for ensuring that badges are issued only to qualified applicants, and must account for and manage all active and deactivated badges.

TSA has the statutory responsibility for requiring individuals with unescorted access to secure areas of the airport to be properly vetted, or checked. TSA fulfills this responsibility through its Threat Assessment and Credentialing adjudication service, which completes the STAs for applicants and provides oversight of the airports' processes through its Transportation Security Inspectors.

Individuals who pose a threat to airport security may be able to obtain badges and gain access to secured airport areas. We evaluated a database of information on active badges at 359 airports. We identified a number of badges issued with one or more instances of omissions or inaccuracies of key applicant data used for vetting, such as STA status, birthdates or birthplaces. [4] Many of the omissions or inaccuracies pertained to critical information used for vetting. For example, one applicant was listed as having three active badges at three different airports. The applications for this individual reflected three different places of birth: the United Kingdom, Ukraine, and the United States. With inaccurate information on place of birth, TSA was unable to accurately vet the applicant, yet the three airports issued the requested badges.[5]

We believe these problems exist because the design and implementation of TSA's oversight of the application process is limited. Specifically, the agency did not ensure that airport operators have quality assurance procedures for the badging application process; ensure that airport operators provide training and tools to designated badge office employees; and require its TSA Inspectors to verify the airport data during their reviews.

Quality assurance: TSA does not ensure that airport operators have quality assurance procedures to safeguard the completeness and accuracy of the vetted data. For example, TSA does not require, and most airports do not have, different individuals verifying the entry of an applicant's information into the vetting process. Having separate individuals verifying the information

[4] The exact number of discrepancies we identified is Sensitive Security Information and cannot be disclosed in publicly available documents.

[5] We followed up on this individual's information. He is a United States citizen and all three badging application files contained copies of his passport identifying the United Kingdom as his place of birth.

would likely enhance the detection of missing or inaccurate information, such as a missing place of birth or a transposition in a date of birth.

In our audit work, we found an airport that had several procedures in place that could be considered "best practices," such as conducting onsite badge audits annually; using a supervisory review checklist to ensure that at least two agents handle each application; using equipment to check identification; and using local police to run criminal investigation checks on badge applicants.

Other best practices include: (1) one airport used daily system-generated reports to identify and resolve potential problems with active badge holders; (2) another airport had a Memorandum of Understanding with U.S. Customs and Border Protection to have the agency verify all immigration documents before submitting the information to TSA for vetting; and (3) yet another airport used a supervisory review checklist to ensure that at least two agents have reviewed the application for completeness and accuracy.

Training and tools: In addition to the lack of quality assurance procedures for gathering and inputting the applicant data, TSA also does not always ensure that airports are providing their individuals with proper training and tools. For instance, officials at 12 airports visited did not know what happens to the data once they enter it. These officials were unaware of how data entry errors or transposed numbers related to key identifying elements could create vulnerabilities, be exploited, and provide the wrong individuals access to secured airport areas.

TSA also does not ensure airport operator employees are using available tools while performing their duties. Tools such as identification document scanners, ultraviolet lights, and loupes (magnifying lenses) allow employees to more closely inspect a document, which prevents fraud. At 8 of 12 visited airports, these employees had tools available to assist in identifying fraudulent documents, but did not consistently use them. For example, at one airport, there was an identification scanner available, which reads the magnetic strip on a driver's license or state-issued ID to display its validity. One employee admitted to using the scanner only occasionally, but not using the lights and loupes at all.

Inspectors verify data: Regarding the inspection process, TSA Inspectors review the airport badging process during inspections; however, the limited coverage does not ensure vetting information is complete and accurate. Inspectors consult TSA's Handbook and the Performance and Results Information System to use basic questions provided, along with guidance, which is based on regulatory requirements from the CFR and TSA Security Directives. The Handbook does not require Inspectors to verify the information reported to TSA to identify discrepancies with badging information. It simply indicates that the Inspector should ensure that proper documentation has been submitted and returned to the airport operator before an employee is granted unescorted access to secured areas. TSA also does not require Inspectors to review any percentage of files; therefore, inspections of badging office records may be insufficient to determine the airports' compliance with vetting process requirements.

Additionally, Inspectors do not always have direct access to the Transportation Security Clearinghouse database and are not required to compare or cross-reference records. This direct access would not only enable Inspectors to verify records for approved STAs timely and take

immediate corrective action if necessary, but it would increase inspection effectiveness and efficiency.

When our audit findings were presented to airport operators, TSA officials, and Inspectors, more than 100 updates were generated, which airport operators sent to the Transportation Security Clearinghouse. We also provided a list of suspect STAs, which prompted Inspectors to take corrective action at some locations. In fact, Inspectors at one airport revealed numerous badges issued without accurate or complete vetting data and immediately revoked access pending an approved STA.

To this end, unless airport operators implement quality assurance procedures for the badging process, the data integrity and vetting results will continue to be questionable. TSA needs to also ensure that airports are providing airport operator employees with the proper training and tools to perform their assigned duties and responsibilities. Furthermore, the agency's inspection activities must be enhanced in order to identify application omissions or inaccuracies for immediate corrective action.

Covert Testing of Physical Access to Secure Areas of Airport[6]

We conducted covert testing to determine whether TSA's policies and procedures prevent unauthorized individuals from gaining access to secured airport areas. We also identified the extent to which Transportation Security Officers, airport employees, aircraft operators, and contractors are complying with related Federal aviation security requirements. The compilation of the number of tests conducted, the names of the airports tested, and the quantitative and qualitative results of our testing are classified, or designated as Sensitive Security Information. We have shared the information with the Department, TSA, and appropriate Congressional committees.

We identified access control vulnerabilities at the domestic airports where we conducted testing. As a result of our testing, we made six recommendations to TSA. TSA concurred with three recommendations, partially concurred with two recommendations, and did not concur with one. TSA continues to conduct significant work in a number of areas to address our recommendations.

TSA's Efforts to Identify and Track Security Breaches[7]

Based on a request from Senator Frank Lautenberg, we conducted an audit into the security breaches at Newark Airport reported in the media. Senator Lautenberg asked the DHS OIG to review the contributing factors that led to the security breaches, 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, and that we determine whether corrective action had been taken on the specific security incidents.

---

[6] *Covert Testing of Access Controls to Secured Airport Areas* (OIG-12-26)

[7] *Transportation Security Administration's Efforts To Identify and Track Security Breaches at Our Nation's Airports* (OIG-12-80)

Our audit objectives were to determine whether TSA at Newark had more security breaches than at other airports; and 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.

Some of our results, such as the comparison of the number of incidents at Newark to other airports, have been designated Sensitive Security Information and cannot be included in this testimony.

Overall, however, we found that while TSA has several programs and initiatives that report and track identified security breaches, it 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. We determined that only 42 percent of the security breaches we reviewed in individual airport files were reported in TSA's official record, the Performance and Results Information System (PARIS)[8] under any category. Additionally, the agency does not provide the necessary guidance and oversight to ensure that all breaches are consistently reported, tracked, and corrected. Our audit work identified corrective action being taken for only 53 percent of the breaches we reviewed.

While there are varying levels and definitions of security breaches, our audit defined "security breach" as 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. 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.

Security breaches are documented locally by TSA at each airport, and TSA staff is required to report security breaches through 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 determine or evaluate how the TSOC used the information about the security breaches we reviewed.

In its response to our audit, TSA reported 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, to include the Transportation Security Operations Center, the Executive Summary Report, TSA's Management Controls Program, as well as an Assessment Team that TSA formed in March 2010.

TSA concurred with both of our recommendations in this audit report and is taking action to implement the recommendations.

---

[8] PARIS is TSA's internal reporting system and official record of a security incident and it contains 33 categories of possible incidents. In our audit, we focused on incident reports in three PARIS categories — security breaches, improper/no screening, and sterile area security events.

Mr. Chairman, this concludes my prepared remarks. I welcome any questions that you or the Members of the Subcommittee may have.