Statement of Mark Hatfield

Acting Deputy Administrator

Transportation Security Administration

U.S. Department of Homeland Security

before the

United States House of Representatives

Committee on Homeland Security, Subcommittee on Transportation Security

February 3, 2015

Good afternoon Chairman Katko, Ranking Member Rice, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in airport access control at our Nation's airports.

The primary mission of TSA is to reduce security vulnerabilities and to strengthen resilience against terrorist attacks in the Nation's transportation systems, including aviation, mass transit, rail, highway, and pipeline, to ensure freedom of movement for people and commerce. To fulfill this vital mission, TSA employs a risk-based, layered approach to security through a well-trained frontline workforce, state-of-the-art technologies, intelligence analysis and information sharing, explosives detection canine teams, Visible Intermodal Prevention and Response teams, and our industry partners who voluntarily adopt security improvements and comply with regulations. This multi-layered approach helps to ensure that resources are applied efficiently to have the greatest impact in reducing risk and enhancing the security of the traveling public and the Nation's transportation systems.

Access Control

Each day, TSA facilitates and secures the travel of nearly 2 million air passengers at nearly 450 airports nationwide. Numerous entities are involved in supporting safe and secure travel as well as providing amenities such as food, shopping, and other entertainment. Controlling access to sterile, (post-security screening checkpoint) airport areas is a critical part of airport operations. While the sterile area hosts passengers and air crews waiting for flights, it is also the workplace for vendors, mechanics, ground crew, and others employed by the airlines and the airports. Access control is a shared responsibility among many partners, and every airport and airline has a security plan of which access control is an important and necessary element. Airport authorities and the airlines are responsible for developing and executing security plans; TSA is responsible for approving security plans and inspecting for compliance.

TSA's inspections include credentialing, perimeter security and testing of access control systems and processes at airports. Every commercial airport receives an annual security

inspection to include an assessment of perimeter and access controls. TSA analyzes the results of these inspections and assessments to develop mitigation strategies to enhance airport security.

Transportation Security Officers and Inspectors are also deployed on a random and unpredictable basis to screen airport and airline workers as they enter for work within the secure and sterile areas. The screening protocols vary by time, location, and method to enhance unpredictability. This includes ID verifications, and searches of individuals and/or their property, using various technologies and methods in order to detect and deter the introduction of prohibited items. Additionally, airport operators are required to conduct random inspections of employees entering sterile areas, to include ID verification and checks for prohibited items. If employees fail to follow proper procedures in accessing secure areas, they may be restricted from future access, disciplined by their employer, or subject to criminal charges and civil penalties.

TSA has wide ranging authority to pursue inspections of airport security plans. Each airport operator is required to allow TSA, at any time or place, to make any inspections or tests, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with TSA's regulations, security programs, security directives, and other policies. Inspections and audits are conducted by our Compliance Division and, in situations of possible non-compliance, investigations are undertaken by Transportation Security Inspectors. Enforcement Investigation Reports that yield evidence of non-compliance are jointly overseen by the airport's Federal Security Director and by the Office of Security Operation's Compliance Division.

Vetting and Badging Process

In addition to our regulatory role, TSA also conducts security background checks for airport and airline employees through the Secure Identification Display Area (SIDA) badging process. Airport workers are vetted before they are granted unescorted access to the secure area of the airport. TSA performs a Security Threat Assessment (STA) on those who require access to the secure/sterile area of the airport or unescorted access to cargo. When individuals apply for employment with the airport or airline, they submit STA information which is passed through one of several vendors to TSA for adjudication. This includes a check against the Terrorist Screening Database (TSDB). In partnership with the FBI and Customs and Border Protection (CBP), the individual also undergoes a Criminal History Background Check and immigration status check. Once TSA has completed the check, the information is provided to the individual's prospective employer with access either granted or denied based on the results of the STA. TSA also continuously checks all SIDA holders against the TSDB in case there are any changes to their status.

With TSA's Risk Based Security model, similar to what we do with trusted travelers in TSA Pre√ or Known Crew Member, airport workers are vetted before they are granted unescorted access to the secure area of the airport. With the STA, we weed out potential bad actors, which is particularly important given the sensitive areas where many of these individuals work. However, we must balance the importance of conducting checks on employees with the need to facilitate air travel, and so have designed a system of background checks, inspections, and random checks as a risk-based approach to access control.

Studies and Recommendations

In 2011, the Office of Inspector General (OIG) assessed TSA's efforts to identify and track access control at airports, specifically whether TSA had an effective mechanism to identify measures that could be used to improve security nationwide. The OIG found that without an effective mechanism to gather information about all security breaches, TSA was unable to monitor trends or make general improvements to security. The OIG made recommendations to use one comprehensive definition of a security breach as well as to develop a comprehensive program to ensure accurate reporting and corrective actions in breach incidents. As a result, TSA developed a single definition of "Security Breach," and enhanced its oversight system with respect to airport security breaches. TSA now leverages the Performance and Results Information System (PARIS) to accurately report, track, and analyze access control trends. Further, TSA updated airport performance metrics to track security breaches and airport checkpoint closures at the national, regional, and local levels.

In 2008, TSA conducted a study to compare two approaches to physically screening airport employees: screening 100 percent of airport employees or conducting random screening measures. Three airports tested the 100 percent screening model and another four screened employees on a random basis. The Homeland Security Institute (HSI) independently assessed the pilot programs using three factors: screening effectiveness, effect on airport operations, and cost considerations. HSI concluded that 100 percent physical screening of all airport employees is cost prohibitive and poses a wide range of operational challenges. For instance, many employees wear steel-toed shoes for safety at work; however this poses a unique challenge and delay in screening through a magnetometer. Additionally, airports conducting 100 percent screening reported delays, ranging from minor at smaller airports to major at larger ones.

HSI also determined that random is nearly as effective as 100 screening, stating that they "did not see a clear distinction between the number of items confiscated at 100% versus random screening airports." Given the HSI and TSA pilot results, TSA made the following recommendations for airports to enhance access control security:

- Accelerate the installation of closed circuit television and perimeter intrusion detection systems;
- Raise physical screening levels for airport employees (TSA and airport operators);
- Phase in the use of biometric access controls and identity verification systems;
- Focus on locally driven security solutions (Community Policing and Airport Watch);
- Increase security awareness training for airport workers;
- Increase Visible Intermodal Prevention and Response teams and surge operations (random and threat-based); and
- Promote behavior-based threat detection programs.

In 2009, the Government Accountability Office (GAO) addressed the issue of insider threats in a review of TSA's efforts to secure commercial airport perimeters and access controls. Using data from the 2008 tests referenced above, GAO reported that physically screening 100 percent of employees would range from $5.7 billion to $14.9 billion for the first year, while the costs of enhancing random worker screening would range from $1.8 billion to $6.6 billion. This audit, entitled *A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, provided five recommendations to further TSA's efforts to enhance the security of the nation's airports through a unifying national strategy that identifies key elements, such as goals, priorities, performance measures, and required resources. TSA concurred with and implemented the recommendations of this audit.

Insider Threat Mitigation

In December 2014, an investigation revealed that a Delta airlines employee allegedly conspired to smuggle firearms from Hartsfield-Jackson Atlanta International Airport (ATL) to John F. Kennedy International Airport (JFK) in New York, and a federal prosecution is underway in this case.

To reduce risks exposed by this criminal conspiracy, TSA has implemented a variety of measures and is examining how this case can inform airport security more broadly. As described above, TSA administers Security Threat Assessments for all airport and airline employees prior to the issuance of SIDA badges granting unescorted access privileges. TSA also vets these individuals on a recurring basis against the Terrorist Screening Database. At ATL and nationwide, TSA requires the airport authority to randomly perform physical screening of employees with SIDA badges at a variety of unpredictable locations such as Secure Area access points, employee bus stops, employee turnstiles, and airport entry gates. In calendar year 2014, TSA performed 7,234 hours of such screening at ATL and 257,979 hours nationally.

TSA has taken immediate steps at ATL to mitigate the insider threat. Under the leadership of TSA officials, a working group was created with representation from various airport authorities, law enforcement, and stakeholders to further develop plans for improving security. TSA has increased operations to focus on screening airport employees at employee entrances and direct access points, such as turnstiles, Secure Area doors and elevators, and vehicle gates. Air carriers at ATL have also implemented additional security measures to address the issue. In partnership with airport authorities, TSA is further examining circulation controls and reassessing employee access points. We look forward to a continued partnership with key stakeholders to determine best practices and risk-based security solutions that could be replicated in other airports.

On a broader level, TSA is examining the potential vulnerabilities exposed by this incident and other trends to determine if additional risk-based security measures, resource reallocations, new investments, or policy changes may be necessary. TSA is conducting an insider threat analysis to identify potential indicators of criminality or threats to aviation that could provide insight into new training, operations, or methods of screening and vetting employees. TSA is examining its legal authorities to assess if additional measures may be required or imposed to enhance security. Finally, TSA Acting Administrator Carraway has asked the Aviation Security Advisory Committee (ASAC) to specifically review access control and perimeter security issues to offer solutions to potential threats.

Conclusion

TSA plays an important role in partnership with airports and airlines in securing access to our Nation's airports, and is committed to fielding responsive, risk-based solutions that can enhance our current security posture. I want to thank the Committee for your interest in this important issue and your support as we consider recommendations and future changes to improve aviation and airport security nationwide. Thank you for the opportunity to testify today, I look forward to your questions.