Statement of Melvin J. Carraway

Acting 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

April 30, 2015

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

In January 2015, I requested that the Aviation Security Advisory Committee (ASAC) convene a working group of industry experts to conduct a comprehensive review of airport access control following the December 2014 incident of a Delta airlines employee allegedly conspiring to smuggle firearms from Hartsfield-Jackson Atlanta International Airport (ATL) to John F. Kennedy International Airport in New York. The ASAC was tasked with examining the potential vulnerabilities for terrorist activities exposed by this criminal incident to determine if additional risk-based security measures, resources, or policy changes were necessary. After a 90-day comprehensive review, the ASAC delivered its report with 28 recommendations to address vulnerabilities at our nation's airports. I would like to report on these recommendations and share with you TSA's next steps in addressing them.

Access Control Background

Each day, TSA facilitates and secures the travel of nearly 2 million air passengers at approximately 440 airports nationwide. Controlling access to the sterile side of the airport, or the area beyond the TSA screening checkpoint, requires finding the right balance between security and the business operations of each unique airport. The sterile area hosts passengers and air crews waiting for flights, but it is also the workplace for vendors, mechanics, ground crew, and others employed by the airlines and the airports, many of whom enter and exit the area multiple times a day as part of their regular duties.

TSA requires each airport to have a security program that includes controlling access to the sterile area, and TSA inspects against these plans to ensure compliance. These inspections include checks of credentialing, perimeter security, exit lanes, employee access, and other critical areas.

Employee Vetting and Screening

TSA has established requirements for security background checks for airport and airline employees who have unescorted access to the sterile area and air operations area. This check is conducted through the Secure Identification Display Area (SIDA) badging process before employees are granted unescorted access to the sterile area of the airport. TSA conducts the name-based portion of the security threat assessment, which includes an immigration status check and recurrent checks against the Terrorist Screening Database. Additionally, under TSA regulations, airports are required to collect and submit fingerprints for a Criminal History Records Check (CHRC) and adjudicate any criminal history data for potential employees.

Individuals who have committed a statutorily-defined disqualifying offense within the preceding 10 years are not eligible for a SIDA badge. While the CHRC is currently a single point in time check prior to employment, TSA has been working diligently towards solutions to provide recurrent vetting of the criminal history data of employees.

Once workers are employed at airports, TSA requires airports to conduct random physical inspections of employees entering restricted areas, including identification verification and checks for prohibited items. TSA also screens workers on a random and unpredictable basis as they enter restricted areas. TSA's screening protocols vary by time, location, and method to enhance unpredictability. Employees who fail to follow proper procedures in accessing secure areas may be restricted from future access, disciplined by their employer up to and including removal, or subject to criminal charges and civil penalties.

Immediate Actions Taken by TSA

In the immediate aftermath of the December 2014 events, I took several steps to strengthen access control security and mitigate the potential vulnerability associated with aviation workers' access to secure areas. These actions include: increasing TSA random and unpredictable screening of airport employees as they enter for work within the sterile area; issuing letters to airlines reiterating that employees on personal travel must be screened at TSA checkpoints; and increasing communication between TSA and our aviation industry partners on threats and potential vulnerabilities.

While these actions can be conducted in the short term, I also recognized the need to adopt long-term solutions and the opportunity to engage stakeholders in the development of

these solutions through consultation with the ASAC, TSA's primary advisory body comprised of industry and security representatives.

Aviation Security Advisory Committee Report

While the measures TSA has in place for background checks, security programs, and compliance inspections provide a good baseline for access control security, the December incident of alleged gun smuggling by an employee with SIDA access illustrated a need to consider additional options to address the potential vulnerability of a terrorist utilizing insider threat methods. Thanks to this Committee's work in passing into law the Aviation Security Stakeholder Participation Act, codifying the ASAC's existence and strengthening its supporting role for TSA's mission, the ASAC was the ideal consultation approach to review access control vulnerabilities. The ASAC's membership of industry, law enforcement, and other key stakeholders brought a broad range of perspectives to the problem of insider threat and access control. The recommendations in their 90-day review are comprehensive, thoughtful, and will help TSA achieve meaningful reforms in partnership with our aviation stakeholders. Additionally, these recommendations use a risk-based approach, allowing resources to be used in the most efficient way for the most effective security.

The ASAC identified five areas of analysis and generated 28 recommendations in each of these areas where TSA and industry can take action to address potential vulnerabilities. These areas are:

- Security Screening and Inspection;
- Vetting of Employees and Security Threat Assessments;
- Internal Controls and Auditing of Airport-Issued Credentials;

- Risk-Based Security for Higher Risk Populations and Intelligence; and
- Security Awareness and Vigilance.

These recommendations focus on activities under the jurisdiction of the TSA granted to it under the Aviation and Transportation Security Act (ATSA, Public Law 107–71 November 19, 2001). The ASAC expects that these recommendations will concurrently mitigate criminal activity in the secured and sterile areas of airports as well.

In terms of security screening and inspection, ASAC recommended that TSA and industry work together to increase the frequency of random and unpredictable screening for airport and airline employees. On employee vetting and security threat assessments, ASAC recommended updating the list of disqualifying criminal offenses and implementing recurrent criminal history records checks for airport and airline employees. Regarding internal controls and auditing credentials, ASAC recommended TSA and industry strengthen policies for proper airport identification media and penalties associated with credential misuse. On risk-based security, ASAC recommended TSA continue to work with our federal intelligence partners and share intelligence information as broadly as possible and appropriate with industry partners. With respect to security awareness, ASAC recommended TSA, industry and law enforcement partners work collaboratively to share best practices and encourage employee engagement on reporting suspicious activity.

The individuals employed by airlines and airports hold positions of trust and as mentioned above are repeatedly vetted against the Terrorist Watchlist. The ASAC recognized the unique role that airline and airport workers may have, including responsibility in securing the airport environment, and recommended leveraging this workforce to its fullest potential. By creating a culture of awareness for all airport employees, through increased training and

promotion of the Department of Homeland Security "If You See Something, Say Something™" program and other initiatives, these employees can serve as a force multiplier and further enhance access control measures.

As a result of ASAC's review, on April 20, 2015 Secretary of Homeland Security Jeh Johnson announced a number of additional steps TSA will take to address the potential insider threat vulnerability at U.S. airports. First, until TSA establishes a system for real time recurrent criminal history background checks for all aviation workers, we will require airports and airlines to conduct fingerprint-based Criminal History Records Checks every two years for all employee SIDA badge holders. We will reinforce existing requirements that all airport and airline employees traveling as passengers are screened by TSA prior to travel. We will direct and work with airports to reduce the number of access points to secured areas to an operational minimum. Additionally, TSA will require airports to increase aviation employee screening, to include additional randomization screening throughout the workday. Finally, we will work with our stakeholder partners to emphasize and leverage the Department of Homeland Security's "If You See Something, Say Something™" initiative to improve situational awareness and encourage detection and reporting of threat activity.

These enhancements to access control nationwide will greatly improve our effectiveness by reducing vulnerabilities and maintaining our risk-based approach to aviation security. Over the coming months, TSA will examine additional recommendations to implement in the future to continue strengthening our nation's airports. I appreciate the ASAC's timely and thoughtful review, and look forward to working with them and our industry partners.

Of note, the ASAC held the consensus opinion that while physical screening of employees is one means of deterring terrorist activity, 100 percent physical employee screening

is not the only, or necessarily the best, solution. Requiring 100 percent physical employee screening would divert limited resources from other critical security functions. Such physical screening, moreover, would require infrastructure improvements, workforce expansion and airport reconfiguration. This would constitute an ineffective use of resources with limited security value. An ASAC working group concluded that "the provision of so-called '100 percent measures' as a layer of airport security does not appreciably increase the overall level of system-wide protection, nor does it lower over-all risk." It concluded that a random and unpredictable screening strategy would be the most cost-effective solution.

For TSA, risk-based security considers how to provide the most effective security in the most efficient way to fulfill our counterterrorism mission and protect the traveling public. As noted by the 9/11 Commission, perfection is unattainable and its pursuit unsustainable. Trying to eliminate all risk results in ineffective security and unnecessarily burdens the aviation industry and government.

Conclusion

Transportation security remains a shared responsibility among government agencies, stakeholders, aviation employees and the traveling public. TSA will continue to apply risk-based, intelligence driven security measures to address vulnerabilities associated with employees who have access to aircraft and secure areas of the airport, while working with industry representatives and the public to strengthen aviation security.

I want to thank the Committee for your continued partnership on this and other important issues, and I look forward to answering your questions.