**Statement of**

**Darby LaJoye**

**Deputy Assistant Administrator**

**Office of Security Operations**

**Transportation Security Administration**

**U.S. Department of Homeland Security**

**before the**

**United States House of Representatives**

**Committee on Oversight and Government Reform**

**Subcommittee on Transportation and Public Assets**

**February 3, 2016**

Chairman Mica, Ranking Member Duckworth, and members of the subcommittee, I am pleased to appear before you today to discuss the Transportation Security Administration's (TSA) role in airport access control and, in particular, aviation worker credentialing at our Nation's airports.

TSA's mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA ensures that airport access control is properly executed in a joint partnership among TSA, airports, air carriers, and other Federal agency partners. To fulfill this critical mission, TSA and stakeholders employ a risk-based security approach that includes: vetting and credentialing of airport and airline employees prior to being granted unescorted access to secure and sterile areas of the airport; the development and execution of security plans as required by Federal regulations; TSA inspections, assessments, and testing of access control systems and processes at airports; and random screening of aviation workers throughout their work day. This multi-capability approach helps to ensure that resources are applied effectively and efficiently to have the greatest impact in reducing risk associated with insider threat.

TSA takes insider threats very seriously and has made progress in addressing such vulnerabilities in America's airports, which were highlighted by the gun-smuggling incident at Hartsfield-Jackson Atlanta International Airport in December 2014. Responding to the Secretary's directives subsequent to that incident, TSA implemented a variety of measures to include: establishing a requirement for airports and airlines to conduct fingerprint-based Criminal History Records Checks every two years for all airport and airline employee badge holders until an automated recurrent vetting solution is identified and in place; reinforcement of existing requirements that employees traveling as passengers be screened by TSA; reduction in the number of access points to secured areas; increase in random screening of employees; and implementation of a joint effort with our stakeholder partners to leverage the DHS "If You See Something, Say Something™" initiative to encourage reporting of insider threat activity. A few highlights of our progress include:

- TSA increased the number of employee screenings from 2.1 million in 2014 to 12.9 million in 2015 over a similar time period.
- Eighty-eight percent of U.S. airports have reduced the number of access points, resulting in an elimination of nearly 500 access points nationwide. TSA is continuing to pursue this initiative.
- TSA's Insider Threat Unit in the Office of Law Enforcement is closely collaborating with Federal and state partners to monitor criminal activity in airports. These actions have led to recent arrests in San Francisco, Dallas, Los Angeles, and Puerto Rico, and demonstrate a renewal of our efforts in this important mission area.

Additionally, TSA continues to implement the recommendations provided by the Aviation Security Advisory Committee (ASAC) on access control and perimeter security at airports nationwide. At the Secretary’s request, the Aviation Security Advisory Committee provided TSA with 28 recommendations to reduce vulnerabilities against an insider threat. Consulting with the ASAC was an extremely productive approach to addressing access control vulnerabilities as their membership, drawn from industry, law enforcement, and other key stakeholders, brought a broad range of perspectives to the problem of insider threat and access control. On April 8, 2015, the ASAC provided its report to TSA, which addressed five security lines of effort:

- 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.

TSA appreciates the ASAC’s timely and thoughtful review. TSA has implemented 10 of the ASAC report’s 28 recommendations and continues to pursue implementation of the outstanding recommendations.

## Vetting and Credentialing of Aviation Workers

Pursuant to statutory authority and regulations, TSA requires airport and airline employees to successfully complete a security threat assessment prior to receiving airport identification (ID) media granting access to non-public areas of the airport.

When individuals apply for employment with the airport or airline, they provide biographic and biometric data information that is used to conduct various security checks. TSA continuously runs the biographic information against the Terrorist Screening Database (TSDB), ensuring there are no ties to terrorism when the individual first applies for ID media and throughout the term of his or her employment at the airport. Also, TSA verifies that all individuals applying for airport ID media have lawful presence in the United States. Individuals who need access to the secure and sterile areas of the airport must also complete a criminal history records check to ensure that they have not committed a disqualifying offense listed in statute within the preceding 10 years. If the applicant successfully completes each phase of the security threat assessment, the airport may issue ID media. Based on security threat assessments, TSA estimates that there are approximately 1.6 million workers with access to SIDA, 1.4 million workers with access to the Sterile Area, and 1.2 million workers with access to Air Operations Area (AOA), noting that an individual worker may be granted access to more than one area with a properly coded badge.

TSA recognizes the value of conducting more frequent, or recurrent, criminal checks on workers to identify cases where there has been subsequent criminal activity since the original application. To date, TSA has been limited in its effort to implement this change because it is not considered a criminal justice agency and does not have access to recurrent criminal checks as are available to law enforcement agencies.

Nevertheless, TSA has pursued other options to gain this capability in a cost-effective manner. In September 2014, the FBI implemented a new automated capability called "Rap Back" that will provide criminal history monitoring services to both criminal justice and non-criminal justice agencies, such as TSA, for a reduced fee. TSA and the FBI are planning to pilot

Rap Back at Dallas/Fort Worth International Airport, Boston Logan International Airport, and at other airports in partnership with Delta Air Lines. The pilot program will provide employers real-time recurrent information on criminal activity committed by credential-holding employees. TSA also recognizes the value of having automated access to additional intelligence-related data in the Terrorist Identities Datamart Environment (TIDE) that may help to further inform TSA's vetting decisions. While TSA can already use this information in manual reviews of SIDA applicants, automated access will contribute to a more efficient STA process and allow TSA to assist the intelligence and law enforcement community based on the findings from the rest of its security threat assessment. TSA, working closely with the Department of Homeland Security and interagency partners, has requested and received approval for this automated access for additional information. This addresses a key Office of Inspector General recommendation. TSA is currently working on the necessary technical changes and policy notifications needed to support implementation and expects to begin receiving automated access to the majority of this data in the coming weeks.

## Development and Execution of Security Plans

While TSA is responsible for conducting the vetting of aviation workers, airport operators are responsible for issuing and managing the ID media that allow individuals to have physical access to secure or sterile areas of the airport. TSA has established security program requirements, based on authorities found in Federal regulations, which airports are responsible to implement and follow. TSA maintains regulatory oversight of airports and conducts inspections to ensure the requirements are being followed. The Code of Federal Regulations, 49 CFR 1542.211 establishes the requirements for an airport authority, describes when they must issue

ID media, how they must account for that ID media, and, in combination with 49 CFR 1542.207, describes the security systems, policies, and procedures that are associated with the ID media, such as reporting lost or stolen ID media, retrieving and deactivating inactive/expired ID media, ensuring appropriate controls on the issuance of ID media, and conducting appropriate audits of the ID media process.

As described above, each airport operator is responsible for both issuing and controlling airport-issued credentials granting access to non-public areas of the airport. These responsibilities are decentralized to each airport, and the number of credentials and the technologies employed for badge recognition at each airport varies. This arrangement allows each airport operator to adjust its security plans for circulation control, consistent with local requirements. It also creates a credentialing enterprise that is more difficult and complex to defeat because of the variety of unique local systems, procedures, and requirements.

## Inspections, Assessments, and Testing of Access Control Systems

TSA's authority to conduct inspections, assessments, and audits of airport access control plans provide a valuable enterprise-wide capability to enforce standards and drive security advancements. TSA requires that airport operators conduct recurring, comprehensive audits of all airport issued ID media and maintain records of those audits for one year, subject to TSA inspection. Individuals granted unescorted accesses are responsible for reporting lost or stolen ID media, and the airport ID systems and procedures must be capable of immediately denying access to any ID media reported lost or stolen. If the percentage of unaccounted for or lost ID media reaches an established threshold for a particular category of access, the airport must reissue all badges in that access category.

The Compliance Division within my office recently conducted a case review of badge audits for Fiscal Years 2010 through 2015. As part of that review, TSA concluded that only 23 of the nearly 440 federalized airports had exceeded the threshold over this five-year period, and therefore, were required to reissue badges. In addition, in June 2015, the Compliance Division completed a Special Emphasis Inspection of all federalized airports and concluded that the average percentage of unaccounted badges was significantly less than the threshold.

TSA also requires airport operators to implement provisions for controlling entry to non-public areas of the airport, and provide for detection of and response to unauthorized presence or movement in the controlled area. Aircraft operators are further required to prevent unauthorized access to their aircraft. TSA's enforcement mechanisms provide for a range of measures, from collaborating with stakeholders to address corrective actions for violations found during inspections to enforcement actions that include fines.

In 2013, TSA launched the Compliance Security Enhancement Through Testing (COMSETT) initiative to improve TSA and industry collaboration and promote more effective security, including airport access control. COMSETT is a data-driven process based on real-world outcomes of security system tests that reveal insights about vulnerability in near real time at both the local and national level. The COMSETT approach allows regulated entities to be tested initially without regulatory enforcement action, collaborate on best practices, and then retest to ensure compliance. Since the launch of COMSETT, TSA has seen improvements in overall compliance, and the agency continues to deploy these tests to address ongoing or any new vulnerabilities identified.

TSA has undertaken additional improvements in tightening airport access control, through its partnership with the FBI to conduct Joint Vulnerability Assessments (JVAs) of airports. These comprehensive threat and vulnerability assessments are accomplished from an adversary's point of view, with the primary focus on identifying vulnerabilities that extend beyond Federal Regulation compliance and that may directly impact the aviation domain. At the conclusion of the JVA, TSA presents a final comprehensive report to the airport Federal Security Director (FSD) to be shared with pertinent airport stakeholders as an additional capability in our effort to reduce risk and improve an airport's security posture.

## Random Screening of Aviation Workers

In addition to vetting and regulatory measures set in place, Transportation Security Officers and airport authority resources are deployed at random to screen airport and airline workers throughout the work day.

Specific TSA screening measures vary by time, location, and method to enhance unpredictability. Measures include ID verifications and searches of individuals and/or their property to detect and deter the introduction of prohibited items. Furthermore, airport operators are required to conduct random inspections of employees entering secure or 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 subjected to criminal charges and civil penalties.

## Conclusion

Thank you for the opportunity to appear before you today to discuss TSA's capabilities and risk-based approach to mitigating insider threat, including aviation worker credentialing. 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, and continue to work with industry representatives and the public to strengthen aviation security.  I appreciate your interest in this issue and look forward to answering your questions.

Transportation Security Administration

# Deputy Assistant Administrator, OSO Biography

**Darby LaJoye** was named as the Deputy Assistant Administrator for TSA's Security Operations in June 2014. In this position he oversees security operations at more than 400 airports nationwide, including a work force of more than 50,000 employees and a budget of approximately four billion dollars. He is also responsible for regulatory compliance, program planning, and partnering with security operators across all modes of transportation within the nation.

**Darby LaJoye**

**Deputy Assistant Administrator**

**Office of Security Operations**

Most recently, Mr. LaJoye served as the Federal Security Director (FSD) of Los Angeles. His responsibilities included the airports of Los Angeles International Airport (LAX), Ontario International Airport (ONT) and Palm Springs International Airport (PSP), with inter-modal responsibilities throughout Southern California and Hawaii. He managed the largest field staff, with nearly 3,000 employees, and sat on several executive boards, including advisory committees at USC and UCLA. Prior to that, Mr. LaJoye served as the FSD at John F. Kennedy International Airport (JFK) in New York.

He began his career with the TSA in 2002 and was instrumental in the federalization of airports throughout the northeastern and midwestern United States. He served as Deputy Assistant Federal Security Director for Screening (DAFSD-S) at Ronald Reagan Washington National Airport (DCA). While in Washington, Mr. LaJoye served as a TSA Crisis Manager for numerous high profile events including Hurricane Katrina, Hurricane Sandy and the American evacuation of Lebanon in 2006.

Mr. LaJoye served three years as Assistant Federal Security Director (AFSD) for Screening Operations at Raleigh-Durham International and the Eastern North Carolina Airports. Prior to his appointment at JFK, Mr. LaJoye provided executive oversight for all Screening, Regulatory, Law Enforcement, and Intelligence functions as the Deputy Federal Security Director for Security (DFSD-S) in Los Angeles.

Prior to joining the agency, Mr. LaJoye served in the U.S. Army in various Light Infantry and Airborne units. He graduated Summa Cum Laude from the University of Richmond, earning a degree in Human Resource Management with a minor in Leadership Studies. He attended Harvard Business School for Executive Education and has a Master's Degree in National Security Strategy from the National War College.

Mr. LaJoye is married with one child.

**UPDATED**: 20140605

**MAINTAINED BY**: OSO COMMUNICATIONS
Oso.commmunications@dhs.gov