Statement of Jeanne M. Olivier, A.A.E.
Assistant Director
Aviation Security and Technology, Security Operations and Programs Department
Port Authority of New York & New Jersey
On Behalf of the American Association of Airport Executives
Before the House Homeland Security Subcommittee on Transportation Security
"A Review of Access Control Measures at Our Nation's Airports, Part II"
April 30, 2015

Chairman Katko, Ranking Member Rice, and members of the subcommittee, thank you for the opportunity to be with you to discuss airport access control – an important security function that local airport operators have held for decades in accordance with strict federal standards, requirements, and oversight. I am testifying today on behalf of the American Association of Airport Executives, which represents thousands of men and women across the country who manage and operate the nation's airports. I am actively involved with AAAE as Chair of the Association's Transportation Security Services Committee. In addition to my work with AAAE, I currently serve as Assistant Director, Aviation Security and Technology for the Security Operations and Programs Department of the Port Authority of New York and New Jersey. In this capacity, I oversee security operations for New York's Kennedy and LaGuardia airports and for Newark Liberty International Airport and Stewart International Airport.

Mr. Chairman, I want to assure you and members of the subcommittee that airports take recent incidents and the prospect of the "insider threat" in the aviation environment very seriously. Airport executives are working constantly in collaboration with the Transportation Security Administration to enhance the layers of security that exist to identify and address potential threats in the airport environment.

In addition to partnering with TSA to help the agency meet its primary mission of passenger and baggage screening, airports as public entities also perform a number of inherently local security-related functions at their facilities, including incident response and management, perimeter security, employee badging and credentialing, access control, infrastructure and operations planning, and a myriad of local law enforcement functions. These important duties have long been local responsibilities that have been performed by local authorities in accordance with federal standards under federal oversight.

Airport operators meet their security-related obligations with a sharp focus on the need to protect public safety, which remains one of their fundamental missions. The professionals who perform these duties at airports are highly trained and have the first responder duties that I know each and every member of this subcommittee, the Congress, and the country value immensely. From a security and resource perspective, it is critical that these inherently local functions remain local with federal oversight and backed by federal resources when appropriate.

Aviation Security Advisory Committee Working Group Report on Airport Access Control

I also recently served as a subject matter expert on the Aviation Security Advisory Committee's ad-hoc working group to review employee screening and airport access control. I was honored to join my other airport colleagues who also served on the group, including Jan Lennon from Atlanta Hartsfield-Jackson International Airport, Michele Freadman from Boston Logan International Airport, Cedric Johnson from BWI Thurgood Marshal International Airport, Alan Black from Dallas Fort Worth International Airport, and Chief Stephen Holl from the Metropolitan Washington Airports Authority Police Department, as well as staff from AAAE and ACI-NA. In addition to airport operators and airport associations, the working

group was comprised of a broad cross section of industry representatives, including air carriers, airline associations, labor, law enforcement, general aviation, security technology and airport services providers.

In a letter dated January 8, TSA Acting Administrator Mel Carraway asked the ASAC to evaluate the aviation industry's current approach to airport employee screening and to review other risk-based approaches to address potential vulnerabilities related to security in the sterile area, including policy and procedures, industry best practices, technology, and employee training. TSA tasked the working group with providing 30-day, 60-day and 90-day reports. The working group's final 90-day report was submitted to TSA on April 8 after approval by the full ASAC.

The working group's report outlines 28 recommendations that collectively take a risk-based and multi-layered approach to employee screening and airport access control with shared responsibilities across the aviation community, including TSA, air carriers and airport operators. Specifically, the ASAC recommendations cover employee vetting; random security screening and inspection; internal controls and audit of badges; risk based security for higher risk employee populations; intelligence and intelligence sharing; and security awareness and vigilance. I have attached the list of recommendations to the end of my statement.

Due to the interdependent nature of each of the recommendations and the complex variables associated with each one, the working group did not have the time to prioritize the recommendations. Time constraints also limited our ability to provide detailed cost analysis. The working group urged TSA to base any future actions related to employee screening and access control on these community-driven recommendations. The group also made clear its belief that any action taken by TSA should be made through the established regulatory process.

The report contains a discussion and analysis of 100 percent employee screening, concluding that 100 percent physical screening would not completely eliminate potential risks and could divert limited resources from other critical security functions. Recent studies have indicated that implementing a 100 percent physical screening approach would cost an estimated $15 billion annually and could cause significant operational disruptions at many airports**.** As a result, the working group developed their recommendations within the context of Risk-Based Security (RBS), a comprehensive approach to aviation security endorsed by the Department of Homeland Security and TSA.

In this regard, the working group agreed that greater implementation of RBS is essential in continuing to shift the aviation security paradigm in a very positive and meaningful way. RBS replaces the old one-size-fits-all security system that was in place prior to the attacks of 9/11, and it has proven to be a significantly better system because it enables allocation of available resources where they have the greatest ability to reduce risk. It also is driven by identifying those with intentions to do harm.

The working group applied risk management principles in considering aviation's exposure to the insider threat and developed appropriate mitigation strategies within the current and proposed budgetary framework. The working group exercised a RBS approach that employed a systematic process of understanding, evaluating and addressing these risks to mitigate the exposed vulnerabilities and to close any security gaps in airport access control. The risk based system for employee screening or access control encompasses intelligence, employee vetting, RBS based on higher risk populations, security awareness, training and behavior analysis, as reflected in the final recommendations.

On April 20, as a result of the recommendations contained in the ASAC report, DHS Secretary Jeh Johnson directed TSA to take several immediate actions:

- Until TSA establishes a system for "real time recurrent" criminal history background checks for all aviation workers, require fingerprint-based CHRCs every two years for all airport employee SIDA badge holders.
- Require airport and airline employees traveling as passengers to be screened by TSA prior to travel.
- Require airports to reduce the number of access points to secured areas to an operational minimum.
- Increase aviation employee screening, to include additional randomization screening throughout the workday.
- Re-emphasize and leverage the Department of Homeland Security "If You See Something, Say Something™" initiative to improve situational awareness and encourage detection and reporting of threat activity.

Airports and the aviation industry are working collaboratively with TSA to implement these requirements. And, while there may be a difference of opinion on the specifics of the short-term actions from DHS and the recommendations of the ASAC working group to TSA, I think it is important to highlight the success of the overall ASAC effort over the past few months and the opportunity it provides as a model for pursuing security enhancements in the future. Airports are very pleased with the collaboration and feel confident that we will achieve better results quicker by having government and industry work together toward the shared imperative of enhanced security.

As the subcommittee contemplates further engagement and potential action to address the insider threat, we urge you to pay careful attention to the detailed work and recommendations of the ASAC working group. Congress and TSA have rightfully recognized the value of the ASAC and the promise of its approach in achieving real, implementable security enhancements.

Other Industry Efforts - Access Control and Perimeter Security

In addition to my work on the ASAC, I serve on the RTCA Special Committee on airport access control, which in 2014 released the updated standard for airport access control (RTCA DO230-D). The document was prepared under the auspices of RTCA, which serves as a Federal Advisory Committee, and provides a vehicle for Federal regulators and regulated parties to develop consensus-based guidance and standards documents.

Notably, the RTCA document provides guidance on acquiring and designing airport security access control systems, testing and evaluating system performance, and operational requirements. It also incorporates the latest technological advances in security access control system and identity management. The major areas covered include: Credentialing; Biometrics; Physical Access Control Systems (PACS), Perimeter Intrusion Detection Systems (PIDS); Video Surveillance Systems; Security Operations Centers (SOC); Integrations; Communications Infrastructure; and General Acquisition Related Considerations.

The 2014 document was the fourth version since the first standard for airport access control was published by RTCA in 1996. The Special Committee has spent the last year working on yet another update – no other airport security standard is updated so regularly. Like ASAC, the RTCA process involves the airport and aviation community working with TSA to provide consensus recommendations and a comprehensive set of guidelines on all technical aspects of access control. The document provides both TSA and airport operators a convenient source of information on current practices and procedures and unbiased information on new technology.

The comprehensive guidance document also contains an entire section on perimeter intrusion detection, which reviews options from patrols to state-of-the-art technology solutions and what factors airport

operators need to consider when implementing a perimeter security solution at their facility. I would be pleased to discuss this important work with the committee in more detail.

Mr. Chairman, airport executives are working constantly in collaboration with TSA to evaluate and enhance the layers of security that exist to identify and address potential threats in the airport environment, including extensive background checks for aviation workers, random physical screening of workers at airports, surveillance, law enforcement patrols, robust security training, and the institution of challenge procedures among airport workers, to mention a few.

In our view, the best approach to enhancing access control at the nation's airports moving forward lies with continuing to focus on robust background checks, maintaining our multi-layered security approach, and preserving and protecting the critical local layer of security that airports provide with credentialing, access control, and other local functions. Inherently local security functions should remain local with federal oversight and backed by federal resources when appropriate.

Members of the committee, recent events have highlighted the fact that we can never rest when it comes to airport security. Airport operators take their responsibilities in this area very seriously and are constantly seeking better approaches in close collaboration with our partners at TSA. I am confident that we can find productive ways to move forward, and I can assure you that the airport community is eager to partner with the subcommittee and all of you to achieve our shared goal of ensuring the highest level of security for the traveling public.

FINAL REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE'S WORKING GROUP ON AIRPORT ACCESS CONTROL RECOMMENDATIONS

Security Screening and Inspection

1. DHS should immediately shift existing resources, as needed, to expand the TSA's random employee screening/inspection program (i.e. the Playbook to secured area access points).

2. TSA, in coordination and collaboration with government and industry subject matter experts and airport and aircraft operators, should develop an employee access security model using intelligence, scientific algorithms, and risk-based factors. This model should give all employees the expectation that they are subject to security screening/inspection at any time while working at an airport.

3. TSA should establish risk-informed, enhanced random screening/inspection for all employees, which would be increased on the basis of identified risk.

4. DHS should request from Congress needed funding for implementation of security measures for a to-be-developed employee access security model and the Playbook.

5. Airport and aircraft operators should prominently post signage at access portals or via other means to alert employees that they will be subject to screening/inspection in order to support compliance with random screening/inspection programs.

Vetting of Employees and Security Threat Assessment

6. TSA should accelerate the implementation of the FBI/Next Generation Identification (NGI) Rap Back Service with an immediate pilot with airport and aircraft operators with a goal of full implementation by the end of CY 2015. Real-time recurrency should be part of the CHRC vetting process, similar to the perpetual vetting conducted by TSA for the STA.

7. TSA should review the existing list of disqualifying criminal offenses to ensure that it is comprehensive enough to address the current threat environment and pursue any legislative or regulatory changes needed to update the list of disqualifying criminal offenses, other eligibility criteria, the addition of permanent disqualifying criminal offenses, extending the look-back period, and starting the period of adjudication on the individual's sentence release date or program completion date.

8. Airport and aircraft operators should introduce new certification language for badge applications that broadens the focus from existing regulatory requirements to a greater focus on overall suitability.

9. Airport and aircraft operators, in coordination with TSA, should review current training for Trusted Agents and Signatory Authorities and, as needed, provide enhanced training on identification documents, identity fraud, and behavioral analysis.

10. TSA should create and maintain a national database of employees who have had their airport- and/or aircraft operator-issued badges revoked for cause.

11. A comprehensive review should be conducted by the TSA to enable a web-based portal for industry utilization for employee vetting by TSA.

12.TSA's Security Threat Assessment should be enhanced to include SSN, running all U.S. citizens against SAVE, fingerprints against DHS' IDENT system, TSA Pre✓® Disqualifying Protocols, and run foreign nationals and foreign-born against international databases.

Internal Controls and Auditing of Airport Issued Credentials

13. TSA, and airport and aircraft operators should assess the efficacy of the auditing program requirements for airport-issued identification media (e.g., security badges) designed to ensure the integrity, accountability, and control of security media.

14. In cooperation with airport and aircraft operators, TSA should consider the establishment of biometric standards which may be used in identity verification and badge validation. Included in this effort should be recommended standards and a cost/benefit analysis focused on implementing any such standards.

15. TSA should implement direct enforcement requirements upon authorized signatories associated with non-compliance, to include failure to immediately report lost, stolen, and unaccountable employee badges and employee separations.

16. Airport operators, in conjunction with tenant business partners, should identify opportunities to further restrict access privileges and/or further reduce access points as operationally necessary.

17. TSA, in coordination with airport and aircraft operators, should support the enhancement/expansion of CCTV or other measures to monitor employees at certain entry points and other areas, as necessary.

RBS for Higher Risk Populations and Intelligence

18. To foster the effectiveness of employee screening/inspection, TSA should consider the development of risk matrices for various employee groups using RBS principles.

19. TSA should maximize the dissemination of sensitive and classified intelligence collection as widely as practicable.

20. TSA should further explore the use of social media to track and assess emerging threats that may pose a risk to aviation. Analysis and best practices gained from this effort should be disseminated to regulated parties.

21. TSA should expand/improve the existing City and Airport Threat Assessment (CATA) or similar program to capture, quantify, and apply applicable intelligence information, and engage the aviation community in developing mitigation measures.

22. TSA should partner with airport and aircraft operators in conducting the Airport Risk Evaluation (A.R.E.) and provide the results of any and all risk and vulnerability assessments to appropriate regulated parties within the aviation community.

23. TSA should further analyze applicable insider-threat cases to create a model of predictive risk factors based on research and applied knowledge of the involved individuals and techniques used to circumvent security measures.

24. TSA, FBI and CBP should provide and make available enhanced training and information on insider threat activity and suspicious indicators that could be incorporated into airport and aircraft operator training programs.

Security Awareness and Vigilance

25. TSA should consistently provide briefings to airport and aircraft operators on the results of their security assessments to provide awareness of potential risks at the airport.

26. Airport and aircraft operators should be encouraged to develop and implement employee engagement/recognition programs aimed at promoting employee engagement in aviation security.

27. TSA, and airport and aircraft operators should promote existing national anti-terrorism reward/employee engagement programs to increase security awareness and reporting of suspicious activity.

28. TSA should promote or establish an existing or new Anonymous Tip Line to receive information from aviation employees who report a security concern or incident, and direct it to the appropriate regulated party(ies).