



**TESTIMONY OF GREG PRINCIPATO, PRESIDENT,
AIRPORTS COUNCIL INTERNATIONAL-
NORTH AMERICA**

**Hearing on
AIRPORT SECURITY: THE NECESSARY IMPROVEMENTS
TO SECURE AMERICA'S AIRPORTS**

April 19, 2007

**Before The Subcommittee on Transportation Security and
Infrastructure Protection
Committee On Homeland Security**

Chairwoman Jackson-Lee, Ranking Member Lungren, and members of the subcommittee, thank you for the invitation to appear before the subcommittee today to offer the views of America's airports on airport security and improvements to enhance the systems currently in place. As the President of Airports Council International – North America (ACI-NA), I am testifying today on behalf of the local, regional, and state governing bodies that own and operate commercial service airports in the United States and Canada. ACI-NA member airports enplane more than 95 percent of the domestic and virtually all the international airline passenger and cargo traffic in North America. Nearly 400 aviation-related businesses are also members of ACI-NA.

Madam Chairwoman, we commend you for holding this important hearing. Each day, airports work to ensure that our facilities are safe and secure for passengers and employees. To this end, airports partner with airlines, tenants, the Transportation Security Administration (TSA), and Federal, State, and local law enforcement to maintain and develop a comprehensive, layered security system that can quickly respond to new and evolving threats. A critical part of this wide-ranging structure is ensuring that individuals with access to secure areas are screened as part of a risk-based security regime that makes the best use of TSA and airport resources.

Before additional security measures are mandated it is important to understand the multi-layered system currently in place for individuals with access to the secured areas at airports. First, persons employed by the airport, airlines or other tenants seeking unescorted access privileges within the controlled areas of airports must provide the airport sponsor with two forms of government-issued photo identification, be authorized to work in the United States of America, and undergo a fingerprint-based FBI criminal history records check to ensure that they have not committed any of an explicit list of crimes designated by Congress during the prior 10 years.

Some airports, with TSA approval, have implemented more rigorous background check standards, verifying information for the past 20 years. Further, at the time of initial employment and throughout the period where access privileges are authorized, these individuals are continually checked against the federal terrorist watch lists developed by TSA, the Department of Homeland Security (DHS) and the intelligence agencies. In addition to the criminal history

records verification and terrorist watch list checks, the TSA conducts a security threat assessment (STA) to verify the individual's identity, employment eligibility and citizenship status.

Access control systems are also an important component in ensuring airport security. These systems have been in place for many years at airports and range from key or cipher locks to sophisticated, fully automated systems utilizing biometric data. The components provide security beginning at the public area through the security identification display area (SIDA). All certificated airports designate these zones in their Airport Security Plans (ASPs) and implement measures to restrict access to those with an operational need to enter the area. Airports must also immediately report to TSA any change in an individual's badge status to ensure that individual's access to the secured areas of airports will be revoked.

Most access control systems are also supplemented by closed circuit television to allow monitoring of the critical areas from a centralized control room, audible alarms to annunciate breaches, and patrols by public safety and law enforcement personnel. Vehicles and equipment seeking access to these areas are inspected by local law enforcement or specially trained public safety personnel. Some new generation access control systems allow for tracking of authorized vehicles within the secure areas.

Airport, airline and tenant employees undergo initial and recurrent security training, specifically tailored to the airport. The training emphasized the individual's responsibilities and duties while working in the secured area of the airport, including the importance of challenge procedures and quickly contacting airport authorities of unusual activities or possible threats.

Additionally, the TSA Aviation Direct Access Screening Program (ADASP) subjects employees and their property to random-screening as they enter the secured area. It is well established that random security checks provide an effective deterrent to both criminal and terrorist activities. Anywhere on the airport at any time, employees know they may encounter TSA screening. We believe that random checks under the ADASP make airport security unpredictable, thus making it difficult for terrorists to ascertain operational patterns that can be exploited.

ACI-NA has been working with TSA, the American Association of Airport Executives and our airport members to develop programs for even more robust employee screening. The program under discussion would not replicate the stationary process currently in place for passengers and their baggage, as the work environment for airport workers has different security issues that must be addressed with measures targeted to meet those potential vulnerabilities. Instead, it includes the use of behavioral recognition techniques and interviews before employees enter the sterile and security areas, targeted physical inspections, enhanced employee training to raise awareness of suspicious behavior, development of a certified employee program, expansion of the use of biometric access controls and deployment of additional airport surveillance technology. ACI-NA recommends that a pilot program using these techniques be conducted for at least 180 days, to assess the improvement in aviation security, the impact on airport and airline operations and the costs of the program. Assuming Congress appropriates the necessary funds to implement the plan, a phased deployment of the program to the 452 commercial U.S. airports could then occur.

Implementation of this six-point program would incorporate the latest intelligence information to allow more nimble and effective security measures, which could be modified quickly to address new and emerging threats. Such a program would also allow different combinations of programs and technologies to be evaluated to determine which provide the greatest security benefits and which are appropriate for airports of varying sizes and configurations.

As you know, Miami International Airport and Orlando International Airport have already implemented a different approach for employee screening. We understand the circumstances which lead to these ACI-NA member airports establishing measures tailored to their unique environment and security challenges. ACI-NA supports the right of airports to exceed federal or state regulatory requirements if they believe the additional security procedures and/or equipment provide a benefit for their passengers and employees.

I want to again emphasize that airports are committed to working with Congress to enhance the already effective airport security system with risk-based measures. We believe that a risk-based program, developed collaboratively by airports, airlines and TSA, will enhance the security of the traveling public by strengthening employee screening while appropriately using resources across the industry.

The members of ACI-NA and I thank you for inviting me to testify today and we look forward to continuing to work with you on this important issue. I'll be pleased to address any questions you might have.