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

**TESTIMONY OF**

**KIP HAWLEY**
**ASSISTANT SECRETARY**

**TRANSPORTATION SECURITY ADMINISTRATION**
**THE DEPARTMENT OF HOMELAND SECURITY**

**BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES,**
**COMMITTEE ON HOMELAND SECURITY**
**SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION**

**APRIL 19, 2007**

Good morning, Chairwoman Jackson-Lee, Ranking Member Lungren and members of the subcommittee. I am pleased to appear before you today to discuss airport security.

At every airport security requires partnerships. TSA, airlines, airports, law enforcement and passengers must work together. Only through cooperative partnerships are we able to provide a robust security system. But airport security is only one layer of security in a larger security system whose mission is to reduce the risk of emerging threats to the entire transportation system.

Aviation security begins well before a passenger arrives at the airport.

1. U.S. government agencies work with others around the globe to identify and disrupt terrorist activities at their source.

2. Customs and Border Protection activities further identify potential terrorists and bar their entry into the United States.

3. Federal, State, and local law enforcement work together with the FBI in Joint Terrorism Task Forces across the United States to identify and disrupt terrorist activities within the U.S.

4. A No-Fly system is used to prevent anyone known to an agency of the U.S. government to be a threat to commit a terrorist act from flying into or in the United States.

5. Airline flight crews and airport employees who have access to an aircraft are subject to an even stricter vetting standard than the No-Fly analysis.

These first five security elements mean that anybody known to U.S. intelligence or law enforcement agencies as a terrorist or a close terrorist associate never gets close to an airplane. But there is much more.

6. An additional, risk-based computer-assisted pre-screening of passengers is conducted before a boarding pass is issued.

7. Hundreds of canine teams and local law enforcement officers are working at airports across the country to identify suspicious articles or people.

8. Surveillance activities take place in and around the airport environment on a daily basis. In 31 airports today, specially trained Behavior Detection Officers look for suspicious behavior.

All of this happens before a passenger even shows up at a TSA checkpoint.

9. At the checkpoint, a professional, well-trained, experienced team of Transportation Security Officers (TSO), assisted by multiple technologies, screens passengers and their carry-on bags for weapons and explosives.

10. In the baggage area, similarly well-trained, experienced Transportation Security Officers use a variety of technologies to screen baggage, and, when necessary, they physically search baggage to resolve anomalies.

Then, on the aircraft:

11. Thousands of Federal Air Marshals fly undercover on a very significant number of flights, both domestic and international.

12. Thousands of pilots who undergo special training and become Federal Flight Deck Officers are authorized and ready to protect the cockpit with firearms.

13. Other local, State, and Federal law enforcement officers travel armed as part of their normal duties and are prepared to intervene.

14. Hardened cockpit doors prevent unauthorized access to the flight deck.

15. And sitting on every airplane are passengers who remember the courage and commitment of the men and women on United Flight 93, and who are prepared to act, if necessary.

Each and every one of these 15 security layers is important.

Relying solely on security at the checkpoint or focusing all of our resources to defeat one threat is counterproductive and detracts from our overall mission. The 9/11 Commission recommended a layered security system saying: "No single security measure is foolproof. Accordingly, the TSA must have multiple layers of security in place to defeat the more plausible and dangerous forms of attack against public transportation." (p.392).

Control of access to sterile and secured areas is just one of the many aviation security layers we have in place. We recognize that, despite our efforts to make each layer as strong as possible, a concerted effort directed at any one layer could be successful. But there is tremendous power in the reinforced, multiple layers. Truly, the whole is greater than the sum of the parts -- and, together, they are formidable.

This plan is more rigorous than 100 percent machine screening of employees at a stationary checkpoint. Because airport employees move about the facility and are not confined to a sterile area (as are passengers), they have access to items throughout the airport and to items introduced at the perimeter. The idea is not to check all employees at specific, known locations, but to check them throughout the facility, to discern hostile intent, to track their movement patterns, and to train employees to detect suspicious behavior. An added dimension of this plan is to narrow the field of employees that we need to know more about on a regular basis. We can do this by creating a level of "certified employees" who have been subjected to a more rigorous, initial level of scrutiny on a voluntary basis and remove them from the regular, but not random screening regimen.

**Employee Background Screening**

Today, someone working in a sensitive airport environment undergoes extensive review before being allowed unescorted access. Airports must submit fingerprints for each individual who is employed or performs duties in the Security Identification Display Area (SIDA) or the sterile area at our Nation's airports. The fingerprints are used to conduct a criminal history records check to ensure that the airport does not grant unescorted access to individuals whose background reveals a disqualifying criminal offense. TSA also conducts name-based security threat assessments of the name against its terrorism and other Federal databases of these individuals as well as anyone with an airport-issued identification medium that allows access to these areas. Any name that is a possible match to a database is referred to appropriate law enforcement or intelligence agencies to determine whether the individual's identity can be verified, and whether the individual continues to pose a threat. TSA informs airlines or airports if an individual's access to secure areas must be denied or rescinded. TSA will soon increase the scope of the Security Threat Assessments to include any individual who holds or is applying for airport-issued personnel identification medium. The Security Threat Assessments of all identification medium holders are conducted on a perpetual basis.

Generally, in order to access sterile or secured areas, anyone who has not been issued a Security Identification Display Area (SIDA) badge for a particular airport, including airport and airline personnel, vendors and contractors, and even TSA employees, must

pass through the TSA security screening checkpoint and submit to the same physical screening process that passengers must pass through before boarding an aircraft.

Airport operators are responsible for developing and implementing TSA-approved airport security programs procedures and processes to control access to sterile, secure and SIDA areas. These programs must include badging, a challenge program, and a compliance regime. All entrances must be secured, and this is generally accomplished by guards or with electronically controlled locks. Nearly 1,000 TSA Aviation Security Inspectors ensure that airports and air carriers comply with the regulatory requirements. In addition, although individuals with a SIDA badge are not required to pass through a screening checkpoint in order to access SIDA areas, TSA, for some time now, has been conducting physical screening of individuals and vehicles entering SIDA areas on an unpredictable basis at numerous airports.

By building unpredictability into our screening and oversight operations, deploying new technology as it becomes available, and utilizing all of our resources more flexibly, we can continue to improve the formidable system of layered security that now exists.

**Aviation Direct Access Screening Program (ADASP)**

In July 2006, TSA implemented the first version of the ADASP that requires screening of airport employees, their accessible property and vehicles upon entering a direct access point screening location for identification, prohibited items and items of interest. Again, while I cannot discuss all of the operational details of ADASP in this setting, I can tell you that the program emphasizes the random and unpredictable aspect of our approach to security. Its scope can take in all or some components of airport security to include gate screening, SIDA identification, cargo or the aircraft itself. Its specific focus, location and duration remain dynamic. It may also include assisting airport and aircraft operators in the performance of their security responsibilities. With our current personnel policies, we are able to surge these activities, as in Orlando, on very little notice.

**Recent Incident at Orlando**

On March 5, 2007, TSA ordered a Delta flight from Orlando to San Juan to be reverse-screened upon arrival, based on information that there were potentially weapons onboard the aircraft. An individual carrying 14 weapons and eight pounds of marijuana was apprehended upon deplaning in Puerto Rico. TSA coordinated efforts between Orlando and San Juan that included local police in both jurisdictions and the FBI. Because an investigation is still ongoing, there is a limit to what I can say in this setting.

The incident, however, raised regional and national awareness of the employee "insider threat" at our nation's airports. TSA quickly deployed more than 160 transportation security officers, aviation security inspectors, Federal Air Marshals and other personnel to augment already existing employee and passenger security efforts.

**Shared Responsibility**

TSA recently expanded its ADASP through Saturation Security Teams (SST) at airports in the region including Orlando, Miami, Fort Lauderdale, Tampa and San Juan. In addition to ADASP, the teams employed behavioral observation techniques, aviation security inspections and other demonstrations of random-continuous security. This operation was marked by a sharp increase in random, unpredictable screening of employees in secure areas. Access to secure areas was limited during non-business hours and door access during those hours was audited for suspicious activity. We deployed integrated teams of Federal Air Marshals, K-9 teams, law enforcement officers and transportation security officers to areas throughout the airport. We conducted random screening of employees and passengers at boarding gates, including using behavior observation techniques, and we randomly inspected aircraft.

The recent surge illustrated TSA's ability to implement random, unpredictable security enhancements anywhere in the nation on short notice. Surges are now a permanent part of our security posture and could occur anywhere, at any time, as part of our unpredictable approach.

This mobilization illustrates TSA's ability to quickly and unpredictably deploy assets based on risk. The agency has developed a longer-term, sustainable plan with our airport and airline partners not only for the Florida/Puerto Rico region, but for the entire U.S. aviation system. TSA will conduct additional operations in other regions in the coming weeks and months on an unannounced basis. Finally, with regard to TSA's workforce at Orlando, several new measures have been established that will further tighten security at Orlando.

At the request of Greater Orlando Airport Authority (GOAA), TSA has entered into a 90-day agreement to take over employee screening at the SIDA access doors in the passenger terminal in exchange for GOAA taking over non-security functions that TSA previously provided. Additionally, GOAA has entered into a contract with a private provider to conduct employee screening at the vehicle checkpoints. While TSA advocates a multi-layered approach to security, we are willing to assist our airport partners in Orlando to meet their goal on a short-term basis. Because of the airport's limited number of employee access doors and willingness to provide personnel to conduct non-security functions, TSA is able to come to this agreement without negatively impacting security in other areas or wait times.

**Conclusion**

Overcommitting TSA resources to inflexible, resource-intensive measures is not consistent with our risk-based approach to aviation security. TSA moves resources in a flexible, unpredictable fashion to address both known and unknown threats with a layered security approach.

Airports have primary responsibility for employee screening, with TSA acting as a regulatory authority. This operation, as well as the broader ADASP program, augments airport security already in place.

TSA employs a risk-based approach to security, including roving transportation security officers that search employees, their packages and their vehicles. Every employee should have a reasonable expectation that they could be screened at any time, at any access point within the footprint of the airport. That applies to all airports, not just where a surge is occurring.

I am aware of Representative Nita Lowey's introduction of HR 1413 as well as HR 1690 to require pilot programs for physical screening of airport workers with access to secured and sterile areas of airports. I look forward to working with Representative Lowey and the Subcommittee on this very important issue.

By building unpredictability into our screening and oversight operations, deploying new technology as it becomes available, and utilizing all of our resources more flexibly, we can continue to improve the formidable system of layered security that now exists.

Mr. Chairman, thank you again for the opportunity to testify today. I would be happy to respond to questions.