Testimony of Steven J. Grossman
CEO and Executive Director
Jacksonville Aviation Authority

before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation Security

A Review of Access Control Measures at Our Nation's Airports, Part II

April 30, 2015

Jacksonville Aviation Authority
14201 Pecan Park Road
Jacksonville, FL 32218
(904) 741-2000

Chairman Katko, Ranking Member Rice, and Members of the Subcommittee, thank you for the opportunity to provide the perspective an of airport operator as well as that of Airports Council International – North America (ACI-NA) on airport access control measures.

I am the CEO and Executive Director of the Jacksonville Aviation Authority and a member of the ACI-NA U.S. Policy Board, which is responsible for the formulation and direction of policy decisions arising under U.S. legislative and regulatory matters. As a member of the ACI-NA U.S. Policy Board, I have a profound interest in and advocate for risk-based aviation security initiatives that not only enhance security but also provide airport operators needed flexibility.

The Jacksonville Aviation Authority, an independent government agency created by the Florida legislature, operates the Jacksonville International Airport, Cecil Airport, Jacksonville Executive at Craig Airport and Herlong Recreational Airport.

Located in Florida, Jacksonville International Airport has more than a dozen major airlines and a network of regional carriers that provide some 200 daily arrivals and departures. In 2013, the number of passengers using Jacksonville International Airport (JAX) reached 5,129,212.

Mr. Chairman, the safety and security of passengers, employees and facilities are top priorities for U.S. airports. As such, the Jacksonville International Airport, and airports across the United States, are in full compliance with federal requirements and, continually works with the federal government and airline partners to examine, test, and improve upon the aviation security system to provide the optimal level of safety and security. In partnership with the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), other federal, state and local law enforcement agencies, and airlines, airports maintain a comprehensive, multi-layered, risk-based aviation security system. In my testimony, I have included several suggestions to further enhance airport access control measures.

Employee Screening

As a result of recent criminal acts involving the unauthorized transportation of guns on board commercial aircraft, U.S. Department of Homeland Security (DHS) Secretary Jeh Johnson and TSA Acting Administrator Melvin Carraway requested that the Aviation Security Advisory Committee (ASAC) conduct an "expedient and comprehensive review" of access control measures to address potential security vulnerabilities at airports.

Tasking the ASAC to identify security enhancements was the right approach and ensured collaboration across the industry. ACI-NA, along with representatives of several member airports, participated on the ASAC Working Group on Airport Access Control in the development of substantive, meaningful and risk-based recommendations. Further, the final report accurately recognizes that each airport is uniquely different and one size certainly does not fit all.

In addition, some have called on TSA to mandate that airports immediately implement 100 percent employee screening. As I will outline in my testimony, 100 percent employee screening does not translate to 100 percent security and moving forward with such a mandate is simply the wrong approach.

Although employee screening is one of the multiple layers in the aviation security system, it is not a stand-alone "solution" and should not be viewed as a "silver bullet," and I am in agreement with the risk-based approach identified by the ASAC.

In 2008, Jacksonville International Airport participated, along with other airports, in a Congressionally-mandated employee screening pilot program conducted by TSA. Despite augmented TSA Transportation Security Officer (TSO) staffing drawn from other airports to support 100 percent screening during the pilot program, there was a negative impact on checkpoint screening operations, and significant additional TSO staffing would have been necessary to permanently sustain 100 percent employee screening. Construction was also

disrupted during the pilot and it became necessary to devote resources to screen the drivers and cement vehicles in a timely manner in order to prevent the cement from hardening before it could be delivered.

As occurs routinely at other small and medium-sized airports, employees regularly transit between public and sterile or public and secured areas. At large airports, hundreds of employees transit such areas during shift changes and at other times. Not surprisingly, it was observed during the pilot that the same employees were repeatedly subject to screening throughout the day.

During the 90-day employee screening pilot at Jacksonville International Airport, approximately 121,000 employees (51,000 of which were passengers in about 35,000 vehicles) were screened, but only one prohibited item was discovered.

The costs associated with the implementation of true 100 percent screening of employees at airports in the U.S. are staggering and are estimated to be in the tens of billions of dollars for the first year alone. Given the questionable security benefit of such a costly initiative, and in consideration for the significant impact on aviation operations, 100 percent employee screening is simply not realistic.

As the ASAC appropriately noted in its Final Report on Airport Access Control, there is no system domestically or internationally that "would qualify as 100 percent screening of 100 percent of all airport employees to passenger screening standards." Implementing such a system in the U.S. would necessitate a significant investment of resources that would then be unavailable to address other pressing threats.

A 2008 Homeland Security Studies and Analysis Institute (HSSAI) report – on the pilot program conducted at Jacksonville and other airports – titled, Airport Employee Screening Pilot Program

Analysis, concluded that “a random screening strategy is the more cost-effective solution” for airports.

As identified by the ASAC, there is no perfect security system. The multiple layers of security – which can be routinely enhanced or modified – provide an effective means to secure passengers, employees, and facilities. A clear strength of this type of system is the unpredictable nature of the individual layers of security and the fact that many airport and aircraft operators exceed the baseline security requirements through the implementation of additional processes, procedures and technologies that consider and are adapted to their unique geographic locations and facility designs.

Therefore, multiple layers of security, including enhanced background checks, security awareness training, and random screening of employees, as recommended by the ASAC, are much more effective than a rigid and predictable 100 percent employee screening regime.

Random and Unpredictable Screening

Unlike airport operators, TSA is in the business of effectively and efficiently screening passengers, baggage and employees at airports. A key element of the TSA Playbook program, formerly known as the Aviation Direct Access Screening Program, is the roving teams of TSA Transportation Security Officers, Behavior Detection Officers and Transportation Security Inspectors that conduct random and unpredictable physical screening of employees working in or accessing secured areas. The Playbook program has proven to be very effective in mitigating risk.

Some airports work in close partnership with TSA in support of Playbook operations to close certain access points and funnel employees through the screening locations. The Playbook program mitigates the risk of prohibited items being introduced at the perimeter, which would go undetected under a fixed-point employee screening system. In addition to introducing a high level of deterrence, Playbook provides employees the expectation of being screened at any time,

not just when they enter through an access control point. This type of random and unpredictable screening program represents a formidable layer of security.

Risk-Based, Multi-Layered Security

Several years ago, TSA appropriately identified the need to transition from a one-size-fits-all approach to risk-based, intelligence-driven initiatives that not only enhance security but also increase efficiency. With limited industry and government resources, risk-based security programs – and regulations – are essential, as we simply cannot continue the process of adding new security requirements and deploying new technology to respond to each new threat.

Probably the most significant risk-based security initiative is TSA Pre✓®, the agency's trusted traveler program, which provides expedited screening to travelers who are enrolled and pre-vetted while focusing the most invasive screening resources on those about whom the least is known. This type of risk-based system is absolutely what is needed and TSA should be commended for directing the implementation of this and other risk-based security initiatives.

We also need to commit to an ongoing transition from the one-size-fits-all approach in the regulatory environment to risk-based security measures and regulation. With only limited resources available, it is essential that airports have the flexibility to apply security measures to those areas where they have the greatest ability to effectively reduce risk.

Airport security systems rely on multiple risk-based layers of security implemented in partnership with airports, airlines, and the TSA. While each layer is not designed to be impenetrable, the individual layers have the ability to deter and mitigate potential risks, and when integrated, the multiple layers provide a robust aviation security system that is not only effective but also capable of being readily adapted to address new and emerging threats.

Through the implementation of the risk-based enhancements identified by the ASAC, the current system will be even more effective in mitigating risk.

Employee Background Screening

An essential layer of security is the multi-faceted employee background screening process which is initiated prior to an employee being granted access to the secured area of an airport. In advance of issuing a Security Identification Display Area (SIDA) badge, which provides unescorted access privileges to secure areas, airport operators conduct extensive vetting of employee backgrounds. There are two critical facets of the employee background screening regime that all employees who work in secured areas must successfully pass: a fingerprint-based Criminal History Records Check (CHRC), and a Security Threat Assessment (STA). Upon receiving an application from an employee seeking unescorted access to a secured area, airport operators validate the identity of the individual, collect and transmit their fingerprints and the associated biographic information to the TSA. The biometric fingerprint data is routed by TSA to the FBI for a CHRC. Through the STA process, TSA conducts a threat assessment against terrorism and other government databases.

If the STA reveals derogatory information about the individual, TSA informs the airport operator that they must not issue a SIDA badge granting unescorted access privileges. If at any point thereafter, recurrent STA vetting reveals derogatory information about an employee with unescorted access, TSA will notify the airport operator to immediately revoke their SIDA badge. Similarly, in accordance with existing regulations, when an airport operator discovers, during a review of CHRC results, that an applicant has been convicted of a disqualifying criminal offense within the previous 10 years from the date of application ("look-back period"), they refuse to issue the individual a SIDA badge. A distinct security feature is the ability for airport operators to review each and every applicant's criminal record to make a determination about their suitability for being granted unescorted access privileges.

Although some airports go above and beyond the baseline measures in current TSA regulations and have implemented longer "look-back periods" and/or an expanded list of disqualifying criminal offenses, others are unable to do so due to restrictive state laws. While some airport operators re-submit a portion of the population of SIDA badged employees for a CHRC, it only provides a snapshot of their criminal record as of the date of submission.

As recommended by the ASAC, the "look-back period" should be extended, and, through collaboration between government and industry, a harmonized list of disqualifying criminal offenses should be developed.

Perimeter Security

Airport perimeter security involves multiple layers of integrated processes, procedures and technologies. Although there is no perfect perimeter security system, the multiple layers of security – which airports routinely enhance – provide an effective system to deter and detect potential intruders. While perimeter fencing and controlled access gates are the most outwardly visible layer of security, there are numerous other layers (systems), both conspicuous and inconspicuous, in place at airports to bolster perimeter security.

Frequent patrols of perimeters in the public and secured areas are conducted by airport and airline personnel, law enforcement officers and other representatives. In addition to patrols, employees at airports are trained to identify and immediately report suspicious activities.

Many airports go above and beyond the baseline security requirements for perimeter security, implementing additional processes, procedures and technologies that integrate more effectively with their unique geographic locations and facility designs.

The individuals involved in most of the "breaches" in recent reports were promptly apprehended. Rather than presenting a gaping vulnerability as some would have us believe, this is clear

evidence of the effectiveness of the layered security system in place at airports. In addition, none of the individuals have been linked to terrorism, and the suggestion that terrorists may attempt to breach perimeters is purely speculative and not based on any empirical data.

Airports, in conjunction with representatives of the TSA, the FBI and other federal, state and local law enforcement officials, conduct joint vulnerability assessments (JVA) of their facilities, systems and perimeters. The JVA results, along with the latest intelligence information, are used by airports to direct the application of resources to enhance individual security layers.

An investment in research and development (R&D) of promising perimeter security technology is essential. In order to evaluate the effectiveness in the operational environment, TSA should commission a pilot test at airports of promising technologies identified through the R&D process. These pilot programs would provide valuable information about cutting-edge technologies that could be used to by airports to further enhance perimeter security.

The National Safe Skies Alliance, in partnership with airports, and funded through the Airport Improvement Program, conducts testing and operational evaluations of security technologies designed to further enhance perimeter security and access control. Many airports have deployed the systems tested and evaluated by the National Safe Skies Alliance. The reports, which are available to all airports, provide specific details about the application and functionality of technologies tested under the program and contain valuable information for airports as they make decisions on which technologies may work best at their facility.

Biometrics

Although biometric access control technology can be a potentially useful tool in limiting access or supporting post-incident forensic analysis, such systems are not a panacea and would not have prevented the situation involving the unauthorized transportation of guns onboard aircraft. In addition to being incredibly costly and challenging to integrate with some legacy airport systems, biometric access control systems are susceptible to environmental conditions and contamination

from substances routinely found in the aviation industry. Reports from TSA officials subsequent to a study of biometrics in aviation and other sectors revealed that such systems are not ready for full-scale deployment at airports, and individual airports should conduct a cost-benefit analysis to determine whether to procure and deploy such systems.

Lost Badges

Recent reports about lost and unaccounted SIDA badges failed to accurately characterize the situation and provided no information about the various security processes, procedures and technology specifically designed to mitigate potential vulnerabilities. Many airports go above and beyond TSA regulations and have designed additional features into their SIDA badges and access control systems to address concerns with lost or unaccounted badges. These include requirements for not only a swipe of the badge but also a personal identification number or a biometric to gain access through controlled portals, security features incorporated into the badges and employee training. Some airports have deployed closed circuit television at access portals. In addition, airports frequently re-issue badges to all authorized employees. Upon receiving reports from badge holders of lost or stolen identification media, airports immediately deactivate the badges in their systems. Due to their sensitive nature, other security features incorporated into access control systems cannot be discussed publically.

Security Directives vs. Proposed Airport Security Program Changes

The most effective approach to rulemaking exists when regulatory agencies afford airports the opportunity to comment on proposed changes to their airport security program. Over the years, ACI-NA and airports have participated on various national and international government/industry working groups intended to enhance aviation security as well as improve efficiency. This coordinated process has been very effective in allowing TSA to identify potential threats to civil aviation, and industry to collaboratively develop aviation security enhancements that minimize unnecessary costs and operational impacts at airports.

Although TSA has the ability to avoid the notice and comment process and issue security directives (SDs), this regulatory option should be strictly reserved for situations involving an immediate threat, as was stipulated in the Aviation and Transportation Security Act and current TSA security regulations. Airports do not believe that Congress intended to provide TSA such latitude that it could issue SDs absent or months after an identified threat.

Security Enhancements

Following are five suggestions to further enhance the security of airport access control:

1. Invest in Intelligence

The importance of timely and actionable intelligence information being used to disrupt terrorist plotting and adjust security baselines cannot be emphasized enough. In the aviation industry, history has demonstrated that effective intelligence information and sharing plays a critical role and provides one of the best opportunities to identify potential threats and prevent terrorist attacks. By way of example, the 2006 liquid explosives plot, the 2010 toner cartridge bomb plot and, more recently, the 2012 "improved" underwear bomb plot were all foiled by intelligence information developed and provided to industry by intelligence agencies.

Armed with this type of information, airports make adjustments to security measures to mitigate threats. Therefore, it is crucial to invest in and provide additional resources to the intelligence agencies with the understanding that actionable intelligence information be shared with airports and airlines in a timely manner.

2. Review and Revise Security Requirements

Even today, there continues to be general hesitancy or fear of rescinding long-standing security requirements, even when it is readily acknowledged that they are outdated – because no one wants to be accused of being weak on security. However, it is the very essence of risk-based security to continually assess the latest intelligence information and conduct informed reviews of

security procedures. Based on such a review, adjustments can be made so security measures maximize risk reduction, something that may necessitate shifting or reallocating security resources to bolster other areas. This reallocation of limited resources ensures that they are being applied to those areas where they can most effectively reduce risk.

3. Institute Real-Time Recurrent Background Checks

Unlike the STA process, through which TSA conducts perpetual vetting of employees who have been granted unescorted access privileges, the CHRC is currently a one-time snapshot of the applicants' criminal history. According to the FBI, Rap Back provides "the ability to receive on-going status notifications of any criminal history reported on individuals holding positions of trust." When implemented, this program will provide airports (and airlines) much better and needed visibility into employees' criminal records, allow them to make informed determinations as to the suitability of existing employees and greatly assist in making determinations about whether employees should be allowed to retain their unescorted SIDA access privileges.

As recommended by the ASAC, TSA should ensure the immediate implementation of the FBI's Rap Back program, so that real-time recurrent CHRCs are conducted on SIDA badge holders.

4. Expand Random Employee Screening Operations

As a means to enhance an important layer of security, TSA should further expand its Playbook employee screening program, so that every employee entering or working in a secured area of an airport has the expectation that they will be subject to screening. Airport operators can support expanded Playbook operations by selectively closing access portals in order to route employees through the screening locations.

5. Institute an Airport Security-Focused Grant Program

Although DHS, through its Homeland Security Grant Program, dispenses billions of dollars annually for systems and technology to bolster state, tribal and local preparedness, resiliency and improve security, very little, if any, is allocated to airport operators. As airport operators have

only limited funding that must be prioritized across a multitude of safety, security and operational projects, an airport security-focused grant program would provide readily available funding to support perimeter, access control and other security enhancements.

Conclusion

Jacksonville International Airport and airports across the United States are committed to working with Congress, TSA, FBI, CBP, state and local law enforcement agencies and aviation stakeholders to enhance airport security through the application of risk-based measures. The recommendations identified by the ASAC for multi-layered, risk-based security enhancements provide the best approach to further enhance the security of the aviation system.

Working in coordination with ACI-NA and airports, TSA should make it a priority to move forward with the implementation of the ASAC recommendations to enhance airport security. Through continued government-industry collaboration to enhance security, we can better achieve our mutual goals of enhancing security and efficiency while minimizing unnecessary operational impacts.

Thank you for the opportunity to submit this written testimony.