

Statement of Mark Crosby, A.A.E.
Chief of Public Safety & Security
Port of Portland, Portland International Airport
On Behalf of the American Association of Airport Executives
Before the House Homeland Security Subcommittee on Transportation Security
“Airport Access Control Point Breaches at Our Nation’s Airports:
Anomalies or Systemic Failures?”
May 16, 2012

Chairman Rogers, Ranking Member Jackson Lee, and members of the subcommittee, thank you for the opportunity to be with you today 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 Chief of Public Safety and Security for the Port of Portland in Oregon, a joint port authority that operates three seaport terminals and three airports, including Portland International Airport (PDX). In that capacity, I have overall responsibility for Emergency Management at the Port and manage the Port’s Public Safety and Security Department, which includes the Airport and Marine Security Departments, the Airport Police Department, Fire Department, and the Communications Center. I have also served on the Public Safety & Security Steering Group for Airports Council International – North America. I am a graduate of the U.S. Air Force Academy and serve currently as a Colonel in the Oregon Air National Guard.

Mr. Chairman, I want to assure you and the members of the subcommittee that airports take recent incidents and the prospect of the “inside threat” in the aviation environment 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, 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 the public areas of airports, local law enforcement presence and patrols provide security far beyond what is typically in operation at other potential public targets such as sport stadiums, train stations, or shopping malls.

The title of today’s hearing poses the question as to whether recent incidents are an anomaly or the sign of systematic failure in terms of access control at airports. From my perspective and the perspective of AAAE, the existing access control system at the nation’s airports works well and is continuously improving. It relies on local management of credentialing and access control systems in accordance with strict federal standards, requirements, and oversight; a robust, multi-layered security apparatus; and extensive efforts to identify “bad” people before they are ever given access to security sensitive areas of airports. That is not to say that the current system is infallible or that improvements cannot be made. Airport executives, for example, are aggressively working to enable voluntary migration to biometric-based badging and access control systems at airports as part of an initiative known as the Biometric Airport Security

Identification Consortium. Other efforts to enhance airport access control technology and procedures are underway as well.

In our view, the best approach to enhancing access control at the nation's airports 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 inherently local functions. While some have argued for federalizing virtually all security responsibilities in airports, doing so would add to TSA's already daunting mission and abandon the successful local systems and process in place that have proven effective for decades in enhancing security and ensuring efficient airport operations. From a security and resource perspective, it is critical that inherently local security functions remain local with federal oversight and backed by federal resources when appropriate.

Airports Add a Critical, Local Layer of Security that Must be Preserved and Protected

As you know, airports play a unique and critical role in aviation security, serving as an important partner to the TSA in helping the agency meet its core mission of passenger and baggage screening. The significant changes that have taken place in airports over the past decade with the creation of the TSA and its assumption of all screening duties have been aided dramatically by the work of the airport community, and we will continue to serve as a critical local partner to the agency as it continually modifies its operations with PreCheck and other risk-based approaches to security, which we fully support.

In addition to partnering with TSA to meet its core mission, airports as public entities provide a critical local layer of security, performing a number of inherently local security-related functions at their facilities, including incident response and management, perimeter security, employee vetting and credentialing, access control, infrastructure and operations planning, and local law enforcement functions. These important duties have long been local responsibilities that have been performed by local authorities in accordance with federal standards and subject to 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.

Preserving the Local Role of Airports with Badging and Access Control is Critical

A cornerstone of security within the nation's airports is the credentialing and background check processes that all workers must undergo prior to receiving airport-issued credentials that grant access to security sensitive airport areas. While a relatively new concept in the maritime environment, credentialing tied to strict, federally specified access control has been a key component of security at airports for more than 20 years. I have included a one-page document at the end of my testimony that provides additional details on airport badging processes and requirements.

In the aviation environment, the background check process for workers operates successfully as a federal/local partnership with the federal government holding sole responsibility for criminal history record checks, security threat assessments, and other necessary government checks for prospective workers and with local airport authorities operating and managing enrollment,

credentialing, badging, criminal history background check adjudication and access control systems in accordance with strict federal standards.

The current system for aviation ensures the highest level of security by combining the unique local experience, expertise, and knowledge that exists at individual airports regarding facilities and personnel with federal standardization, federal oversight, and federal vetting assets. Local involvement provides a critical layer of security and gives airports the operational control they require to ensure that qualified employees receive the credentials they need to work in the airport environment.

In contrast to the long-standing locally controlled credentialing and access control apparatus that exists in the aviation environment, the credentialing/access control system in place in the maritime environment with the Transportation Worker Identification Credential (TWIC) program is relatively new. Under the TWIC model, the federal government or its contractors are responsible for virtually all aspects of credentialing, including worker enrollment, applicant vetting, and credential issuance.

Some have suggested abandoning the successful local systems and processes already in place at airports with badging and access control to expand TSA and the federal government's control over more of the process as is the case with TWIC in the maritime environment. Airport executives oppose any move to shift any additional functions in aviation to the federal government and believe that such a move would diminish security by reducing or eliminating a critical, extra layer of security that is already in place in airports.

Pursuing such an approach would scuttle a successful local/federal model that has worked well for decades, eliminate local operational control, stymie significant efforts already under way at airports across the country to upgrade and biometrically enable existing airport badging and access control systems, and significantly increase costs to the aviation industry with no demonstrable security benefit.

While the desire to centralize and federalize the process for all transportation worker vetting programs may be understandable from the federal government's perspective, airport executives are concerned about federal intrusion into existing processes that have worked well for decades. Airports are also very concerned about having to help foot the bill for these initiatives – estimated at \$633 million through 2025 in appropriations and new fees as part of the TTAC Infrastructure Modernization (TIM) program – for changes that provide them with no demonstrable security or operational benefit. The current system in aviation operates efficiently and effectively at a fraction of the cost of other transportation vetting programs and at no cost to the federal government. Airport executives want to ensure that remains the case.

With the federal government and state and local governments operating under historic budget constraints, it makes little sense to devote hundreds of millions of dollars in scarce resources to federalize functions that airports have performed successfully for nearly a decade. The TIM effort fails to take into account the long-proven approach that exists in the aviation industry.

Biometric Airport Security Identification Consortium (BASIC)

Before concluding, I want to take this opportunity to bring the subcommittee up to date on a related topic and the efforts of the Biometric Airport Security Identification Consortium or BASIC initiative. In simple terms, the objective of BASIC is to define a comprehensive, airport-

driven Concept of Operations that will enable voluntary migration to biometric-based badging and access control systems at airports – a goal that I know subcommittee members share. More than 40 airports of all sizes actively participate in BASIC. I would note that BASIC airport participants are working cooperatively with TSA on this initiative as well as with other groups, including the Airport Consultants Council.

Many airport operators – including the Port of Portland – are eager to move forward with biometrics, but concerns remain about the prospect of overly prescriptive and costly solutions. Airports are also eager to avoid repeating mistakes made in the past where the federal government required costly and often proprietary access control systems to be deployed in airports in a compressed period of time. That approach proved both expensive and ineffective.

In an effort to avoid unnecessary regulations and a one-size-fits all mandate regarding biometric-based systems, airports participating in BASIC have identified several key principles that must be part of any future biometric-based badging and access control systems, including:

- Safeguards on local control and issuance of credentials,
- Leveraging of existing capital investments and resources,
- Standards-based open architecture and local determination of qualified vendors, and
- Phased implementation that migrates over time.

In addition to building on the processes and regulations already in place at airports today, BASIC is also working to adapt important federal standards regarding secure biometric credentials into the airport's operational environment. For example, Federal Information Processing Standard (FIPS) 201 and the more recent Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers are reflected throughout the BASIC Concept of Operations and greatly inform the recommended phased implementation for airports.

The BASIC working group, which meets on a regular basis, is moving forward aggressively to update and refine a detailed Concept of Operations that will define the biometric components and common business processes that need to be added to airports' existing procedures to enable biometric-based badge and access control systems in a reasonable and cost-effective timeframe. In fact, several airports have already begun to implement the early phases of the BASIC Concept of Operations. Newark Liberty International Airport, San Francisco International Airport, Aspen Pitkin County International Airport, Los Angeles International and Salt Lake City International Airport – to name just a few – have implemented a secure messaging structure for the submission of biographic security threat assessments and biometric criminal history record checks that will ultimately enable the return of trusted biometrics back to the airport for use on credentials or in access control systems.

Airports are committed to moving forward to bring biometrics into the airport environment as soon as possible in a manner that builds upon existing capabilities and limits operational difficulties. The BASIC initiative, which is being driven by airports in cooperation with the federal government, offers the best opportunity for making the promises of biometrics a reality in a timely manner.

Mr. Chairman, in closing, let me thank you once again for the opportunity to testify today. As an experienced security professional responsible for managing public safety and security operations at airports as well as vibrant maritime port facilities in my home of Portland, I am proud of the

important role that local officials play in ensuring the highest levels of security and safety within critical transportation facilities.

As I have highlighted throughout my testimony, the access control apparatus at airports is unique among other transportation facilities and has operated successfully for decades. Airport operators, which are extensions of local government, are directly responsible for credentialing and access control under strict federal rules and oversight in recognition of the security and operational expertise that exists at the local level. Local involvement provides a crucial, additional security layer that should not be discarded.

The current system in aviation leverages local experience, knowledge, and expertise with federal standardization and vetting assets. Airport operators know and understand their facilities, and they maintain decades-old relationships with the numerous parties that employ individuals throughout the airport environment, resulting in high levels of security.

Abandoning a decades-long record of local expertise and investment in favor of an unproven system under which credentialing and access control would be controlled centrally out of Washington or elsewhere – as is being attempted in the maritime environment with TWIC – would be a huge step backwards in terms of security from where we are now with aviation.

We appreciate your leadership and the work of this subcommittee to preserve and protect the important role that local airport officials play in partnership with TSA to ensure the highest levels of security at their facilities.

I look forward to answering any questions you might have.



Airport Badging Requirements and Processes

Historical Context

Airport operators and the aviation industry have a robust history of credentialing and access control experience. Since the inception of this approach more than 20 years ago, airport operators have been delegated badging authority by the federal government. In the early 1990's airports installed access control systems that for the first time were tied to a credential. In 1996, airports started utilizing criminal history record checks (CHRC) conducted by the FBI to adjudicate employees whose employment backgrounds could not be verified.

Current Requirements and Practices

Since shortly after the September 11, 2001, terrorist attacks, CHRCs have been conducted on all employees with access to the Secure Identification Display Areas (SIDA) and Sterile Areas. Beginning in October 2007, TSA regulations also require name-based security threat assessments (STAs) for all individuals applying for either a SIDA or Sterile Area badge.

The FBI performs CHRCs and provides airports with the full results of an applicant's check. TSA performs STAs, which check an individual against the Terrorist Screening Database and "determines whether there are any outstanding immigration, terrorist or federal open wants or warrants issues pending against the potential employee." TSA provides airports with either "approved" or "disapproved" status for a prospective employee only based on security sensitivities.

Airport operators maintain responsibility for worker enrollment, and badging, issuing local badges with card topography and identifying features unique to that airport facility. By regulation, airport operators and air carriers are responsible for adjudication of the CHRC which allows airport operators to know more about individuals that have access to their facilities. In some cases an individual is not disqualified under CHRC rules; however the individual may require further scrutiny or at least situational awareness for the Airport Security Coordinator. This approach provides a critical local layer of security.

Federal/Local Partnership in Aviation – Unique Among Other Transportation Modes

In the aviation environment, the background check process for workers operates successfully as a federal/local partnership with the federal government holding sole responsibility for STAs and other necessary government checks for prospective workers and with local airport authorities operating and managing enrollment, credentialing, badging, criminal history background check adjudication and access control systems in accordance with strict federal standards.

The current system for aviation ensures the highest level of security by combining the unique local experience, expertise, and knowledge that exists at individual airports regarding facilities and personnel with federal standardization, federal oversight, and federal vetting assets. Local involvement provides a critical layer of security and gives airports the operational control they require to ensure that qualified employees receive the credentials they need to work in the airport environment.



Mark Crosby, A.A.E.

Chief of Public Safety and Security
Portland International Airport
Port of Portland

Mark Crosby is the Chief of Public Safety and Security for the Port of Portland, a joint port authority that operates three airports and three seaport terminals, including Portland International Airport (PDX). Mark is responsible for managing the Port's Public Safety and Security Department which includes the Airport and Marine Security Departments, the Airport Police Department, Fire Department, the Communications Center as well as having overall responsibility for Emergency Management at the Port. Previously, Mark held various positions in operations, security and real estate at the Port and with the airport system in Sacramento, California.

At the national level, Mark is an accredited airport executive (AAE) with the American Association of Airport Executives (AAAE) and serves as the Chairman of AAAE's Airport Security Committee. He also has served on the Public Safety & Security Steering Group for Airports Council International-North America. In these roles, Mark serves on numerous national, policy task forces with both the Transportation Security Administration (TSA) and Federal Aviation Administration (FAA).

Regionally, Mark is a member of the Oregon Governor's Homeland Security Council and the Portland Regional Emergency Management Group as well as a board member of the Northwest Chapter of AAAE.

Mark is also a colonel in the Oregon Air National Guard where he is the Director of the State Partnership Program between Oregon and the nation of Bangladesh. Formerly, he served as the Director of Communications/Information Technology (J6), was the commander of two combat communications squadrons, and was the deputy commander of the domestic terrorism civil support team. He is a graduate of the U.S. Air Force Academy and holds an MBA in Finance from Golden Gate University.