OBAMA-BIDEN TRANSITION PROJECT

THIS DOCUMENT WAS PRODUCED BY AN OUTSIDE PARTY AND SUBMITTED TO THE OBAMA-BIDEN TRANSITION PROJECT.

CrewPASS

Recommendations of the Air Line Pilots Association, Int'l, for Creating CrewPASS

A Biometric-Based Flight Crew Security Screening System

May 2007

alpa

alpa AVIATION SECURITY

STRONG • FOCUSED • SAFE

ALPA

PILOTS IN COMMAND

THIS DOCUMENT WAS PRODUCED BY AN OUTSIDE PARTY AND SUBMITTED TO THE OBAMA-BIDEN TRANSITION PROJECT.

A Proposal for Creating CrewPASS

A Biometric-Based Flight Crew Security Screening System

I. Executive Summary

A current weakness of the U.S. aviation security system is that it may allow uniformed flight crew imposters to pass through passenger security screening checkpoints and illegally gain access to airport secure areas. While passenger screening checkpoints may be adequate for detecting improvised explosive devices and metallic weapons, they are incapable of determining whether someone wearing a flight crew uniform is currently employed as an airline pilot, and is the person he or she claims to be.

Although access control systems are required at Transportation Security Administration (TSA)-regulated airports, and those systems are suitable for identifying and verifying the employment status of domiciled employees, they do not include transient crewmembers.

The Air Line Pilots Association, International (ALPA) convened a small industry working group in February 2007 to develop a proposal to address this security deficiency. This proposal, based on the highly successful and efficient Cockpit Access Security System (CASS), is called Crew Personnel Advanced Screening System, or CrewPASS.

CASS uses the employee databases of participating airlines to electronically confirm the identity and employment status of pilots so that they may gain access to the jumpseats of airplanes belonging to companies other than their own. CrewPASS would extend the CASS concept to discrete crew portals and security screening checkpoints to electronically screen flightcrew members quickly, efficiently, and effectively, thereby addressing the current security deficiency. CrewPASS would not require purchasing or issuing new identification cards; existing airline ID credentials would suffice to guarantee that flightcrew members have passed all required background checks and are employed by a U.S. airline.

CrewPASS is intended to be operated as a prototype and, pending a successful test, become a standing, TSA-operated program. CrewPASS is expected to become a very successful, low-cost and effective example of how government and industry, working together, can improve security and efficiency to the benefit of the traveling public, the airlines, and their employees.

II. Policy Considerations

The TSA's CASS program permits identified flightcrew members to obtain access to the most security-sensitive area of any airport—an airliner cockpit. CrewPASS would permit flightcrew members to obtain access to less security-sensitive areas of the airport, such as the passenger terminal.

CrewPASS would significantly enhance security by providing a real-time match of an employee's photo stored in an airline database with the crewmember possessing an airline ID bearing the same photograph. CrewPASS would virtually eliminate the possibility of a uniformed terror-

ist being processed through screening as an armed flightcrew member.

Section 106(h)(4)(E) of the Aviation and Transportation Security Act (ATSA) reads, in part, "The Undersecretary . . . may provide for the use of biometric or other technology that positively verifies the identity of each employee . . . who enters a secure area of an airport." CrewPASS would be developed and implemented in concert with this Congressional authorization.

The Senate Commerce Committee approved language in February 2007 that was included in the Senate's Aviation Security Improvement Act (S.4) to require the TSA to develop a system to enable crews to be electronically screened at the screening checkpoint (see Appendix 1). This legislation is pending in conference with the U.S. House of Representatives. The House staff members have indicated that this provision will likely remain in the final bill.

CrewPASS would significantly enhance security by providing a real-time match of an employee's photo stored in an airline database with the crewmember possessing an airline ID bearing the same photograph.

The TSA Administrator stated his intentions in May 2006 to provide a biometric credential for crewmembers "as soon as possible" (see Appendix 2). ALPA offers the CrewPASS concept as an identity solution for the Administrator that is (1) highly secure, (2) maximizes use of existing equipment, (3) minimizes cost, and (4) is biometric-based.

Depending on how CrewPASS is ultimately configured, it could require TSA personnel to check crewmembers' identification. The TSA recently indicated that it wants to assume that function from the airlines and asked for $60 million to hire

2,000 federal workers who would check photo IDs and observe passenger behaviors and anomalies.

ARINC and Continental Airlines have volunteered to support development of the CrewPASS prototype. The TSA should bear all installation and operating costs as part of the overall security screening function that it now performs.

The TSA and several aviation industry organizations announced on April 18, 2007, their plans to implement six measures to bolster employee screening by using a risk-based approach (see Appendix 3). CrewPASS could make a solid and immediate contribution to this new initiative.

Random security screening now being conducted at airports will provide an additional layer of security to CrewPASS.

Congress has announced its desire to require 100 percent screening of all airline and airport workers who are admitted to secure areas (see Appendix 4). CrewPASS should go far in addressing those Congressional concerns. If proper identity and employment status are not confirmed for all workers who board or service an aircraft, more expensive and time-consuming measures, such as additional aircraft searches and inspections, could become necessary to ensure that aircraft security is maintained.

The TSA currently permits pilots to gain access to secure areas at several U.S. airports via identity checks at crew-only portals. CrewPASS would permit the expansion of that policy and make such access available at any airport where CASS is used.

III. Background

Airport security screening was established in the United States in the early 1970s as a direct result of the Cuban hijacking crisis. From its inception, the focus of checkpoint screening in the United States was to find potentially dangerous objects carried by passengers that might threaten the security of an airliner, passengers, and flight and crews. Given the type of threat posed in the 1960s and 1970s by homesick Cubans who had no desire to commit suicide and mass murder, this was a rational and quite effective approach.

However, on December 7, 1987, a Pacific Southwest Airlines customer service agent who had been fired used an expired company identification card to bypass a security-screening checkpoint in Los Angeles and board PSA Flight 1771 with a handgun. The fired employee reportedly killed the flight's pilot before the airliner crashed into the ground near San Luis Obispo, Calif.; 43 people died in this tragedy

In response to that event, the FAA amended Federal Aviation Regulation (FAR) Part 108 in 1989 to prohibit airline employees bypassing security screening checkpoints. The FAA also revised FAR Part 107 to require major U.S. airports to install computerized systems, or their equivalent, for controlling access to airport secure areas. The electronic access control systems developed under the broad guidelines of FAR 107.14 relied on a local database to confirm an individual's employment and authorization to enter a secure area before granting access. Regrettably, these systems were not required to be interoperable.

In 1993, Congress appropriated $2 million to develop and implement the Transient Crew Security System, which was designed to make different airport security systems interoperable for the benefit of transient airline crewmembers. The FAA dubbed the prototype the Universal Access System (UAS). The agency successfully developed standards and performed limited proof-of-concept testing at a few U.S. airports with the help of two major airlines from 1994 until 1997. UAS was based on magnetic stripe technology, however, and though some airlines expressed an interest in deploying it, the maturation of "smart" card and biometric technologies in the late 1990s were among the several factors that weighed against doing so.

The tragic events of Sept. 11, 2001, refocused the U.S. government's attention on the need for better worker identity management. The Transportation Worker Identification Card (TWIC) is a biometric-based smart card that began development more than 5 years ago for various modes of transportation. The TSA has not determined whether it will deploy TWIC for use by the aviation industry. The TSA has stated that if TWIC is eventually deployed, any use of the system for the purpose of gaining access to secure areas will be strictly up to the airport operator community; no national policy on its use will be issued.

Despite these events, a genuine security need—that of positively identifying flight crews and verifying their employment status—remains unmet, and the security of the traveling public is being put at unnecessary risk. This proposal, therefore, describes and advocates developing and implementing the Crew Personnel Advanced Screening System (CrewPASS), a biometric-based system that builds on the foundation of the TSA's highly successful CASS.

CrewPASS would provide a much higher level of security than is currently afforded by physical screening of flight crewmembers while lowering costs, enhancing efficiencies, and reducing the length of security screening lines for the flying public.

IV. Leveraging Trust as a Component of Security

Airline pilots are the most heavily scrutinized civilian employee group in the United States. Pre-employment examinations for airline pilots include TSA-mandated criminal history record checks, employment record checks, medical examinations, drug and alcohol tests, psychological examinations, and multiple interviews. Airline pilots are continuously screened for both professional proficiency and demeanor, are subject to repeated criminal history checks, and are continuously exposed to peer pressure and oversight. They must meet stringent professional standards and can be fired even for something as insignificant as failing to reveal traffic violations on periodic physical examination applications.

The hiring of an airline pilot represents the end of a long, arduous journey for many that normally begins with a unique vision coupled with a tremendous desire to meet the challenges necessary to reach the objective. A reasonably high level of formal education is a fundamental requirement for starting a career as an airline pilot. Many airline pilots have had a military aviation background, and many have been commissioned officers, often with top-secret security clearances requiring extensive background checks to determine the reliability and integrity of the candidate. This level of scrutiny continues throughout a pilot's career as he or she meets various access requirements dictated by different locations, job positions, and functional requirements. Civilian-trained pilots meet similar challenges, all over a long period of time.

Airline pilots are continuously screened for both professional proficiency and demeanor, are subject to repeated criminal history checks, and are continuously exposed to peer pressure and oversight.

Airline pilots normally serve a one-year probation, during which time the company may fire the pilot for any cause. New-hire pilots are "under the microscope" by their management and colleagues, but this type of scrutiny continues for the entire period of employment.

Check rides provide opportunities for instructors to examine not only flying proficiency but also other factors that influence potential performance, judgment, and stability. They examine how well a pilot responds to the stress of inflight emergencies in a flight simulator. All U.S. airline pilots are subject to annual line checks by FAA-designated examiners, and new captains must pass check rides with FAA examiners.

All of these factors contribute to the continuous assessment of the relative risk represented by an airline pilot and, as a result, make him or her quite different from other types of aviation employees. Pilots are not security liabilities—they are assets who enhance security and function as inflight security coordinators. They are resource managers who have great concern for the security of flight, primarily for their passengers, but also because their own lives are at stake.

Trust and Verify

Because pilots manipulate their airplane's controls, they literally hold the lives of their passengers (plus those of their fellow crewmembers and those of persons on the ground) in their hands, regardless of whether the pilots have a weapon in their possession. For that reason, genuine security is derived by hiring trustworthy flightcrew members and continually verifying their trustworthiness, but otherwise letting them do their jobs unimpeded by unnecessary constraints. Canada and Israel both follow this philosophy, as is evidenced by their respective pilot security measures. Canada recently instituted the Restricted Area Identity Card (RAIC), which operates in the same fashion as the proposed CrewPASS in that it verifies the identity and employment status of pilots in lieu of physical screening.

Israel has not had an airline hijacking in more than 30 years despite being a primary target of terrorists. The Israeli aviation security system is not based on physical screening of pilots; rather, Israeli authorities trust pilots, but verify that trustworthiness by using tools, training, and tactical knowledge based on generations of experience.

Pilots are an important component of the aviation security system, but the trust that they have earned is ignored when they are required to submit to passenger security screening, for the reasons noted above. This situation has led to a demoralized and frustrated pilot group that has lost confidence in the government's ability to provide reasonable, rational, and effective security services. Instead of being physically screened multiple times each day, pilots should be recognized as part of the security solution, not part of the problem. Physical screening of trustworthy airline pilots, which causes longer-than-necessary screening queues, takes away from time that could be put to better use in screening unknown passengers.

A better way of screening pilots is needed—and CrewPASS is that better way. CrewPASS could also be used to enhance security screening of other employee groups having access to the cockpit. The FAA specifies which groups of employees are permitted access to the cockpit and under which circumstances. As shown in Table 1, flight attendants, mechanics, and other airline personnel may be admitted to the cockpit under certain specific circumstances, always with the concurrence of the captain (i.e., pilot in command).

TABLE 1

Transient Employee Group	Authorized Access to Cockpit?	Authorized to Operate Aircraft in Flight?	Need Dangerous Items to Commandeer an Aircraft?	Appropriate Threat Countermeasures
Pilots	Yes	Yes, per FAR Parts 61, 91 and 121	No	Pre-employment checks to determine trustworthiness Ongoing scrutiny by FAA personnel, medical professionals, airline management and other pilots to continually verify trustworthiness CrewPASS verification
Flight Attendants	Yes, for periods as determined by the captain; no access to cockpit jumpseat	No	Yes	Pre-employment checks to determine trustworthiness Physical screening for dangerous items CrewPASS verification
Mechanics	Yes, may occupy jumpseat with captain's permission per FAR 121.547	No	Yes	Pre-employment checks to determine trustworthiness Physical screening for dangerous items CrewPASS verification
Management Personnel	Yes, may occupy jumpseat with captain's permission per FAR 121.547	No	Yes	Pre-employment checks to determine trustworthiness Physical screening for dangerous items CrewPASS verification

V. Technical Description of CrewPASS

Prototype Version

Shortly after Sept. 11, 2001, the FAA stopped allowing cockpit jumpseat access to flightcrew members except those from their own airline. The TSA reinforced this restriction further and regulated the use of jumpseats through security directives. As a result, flightcrew members who were previously allowed to use jumpseats on other airlines were required to compete for standby seats in the passenger cabin—often without success. To resolve the need to maintain security in the cockpit while allowing interline use of jumpseats, the ARINC Cockpit Access Security System (CASS)—a service approved by both the TSA and the FAA—was developed. CASS not only reestablished reciprocal access to jumpseats, it also improves cockpit security by verifying the identity and employment credentials of persons asking to ride in a jumpseat.

CASS is an operational system that has been used since July 2004 to provide a reliable means of real-time verification of the identity and employment status of airline pilots at the boarding gates of most major U.S. airports. The system is currently used by 68 U.S. airlines that could immediately participate in a demonstration of CrewPASS at selected airports.

CASS enables gate agents to query the personnel records of airline employees wishing to use a cockpit jumpseat. The airline pilot employee provides the gate agent with the prerequisite identification, and the gate agent generates an electronic message requesting cockpit access. The request is then forwarded to the ARINC CASS server, which routes the query to the airline's designated database. The approval or denial response is routed back through the ARINC CASS server, which returns the response to the gate agent's computer terminal.

The CASS response message includes an up-to-date photograph of each employee participating in the program.

In CASS, each participating airline develops, maintains, and houses a database of its own employees who are authorized to fly in the cockpit jump seats of other airlines. This database, known as the Airline Human Resources Database (AHDB), identifies employees by using their passport information and a photo. In addition, each airline uses an Airline Host Requesting System (AHRS) application to generate access request messages and provide the interface between the gate agents and the ARINC CASS server.

For CrewPASS purposes, ARINC proposes to supply an AHRS application to allow access requests to be made on Internet browsers located at selected crew portals and security lanes of the screening area of target airports. This is the simplest and lowest-cost implementation, using existing development and the TSA's own computers.

Biometric Included in CrewPASS

The CASS response message includes an up-to-date photograph of each employee participating in the program. A photograph is considered biometric data and provides a TSA agent with a high level of identity assurance. The photographs allow the TSA agent to immediately verify that the person presenting the airline identification card is currently in good standing with the airline and should be allowed access to the airport gate area.

Portability and Scalability

The equipment required at an airport screening point to use CASS is a PC computer with a web browser (i.e., Internet Explorer or Firefox) and

access to the Internet. Many currently available portable devices, ranging from cell phone to PDAs, could fulfill this requirement.

The current Web-based application would be modified to allow each additional airport, or computer at an airport, to have its own log-in account that would be configured by the TSA.

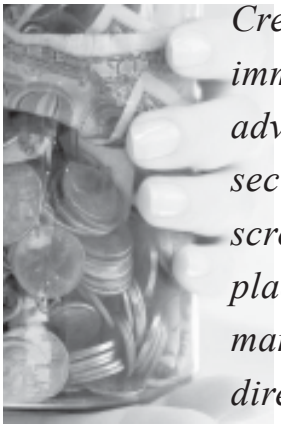
The primary effect on the ARINC CASS system of adding additional airports to the system would be additional message traffic at the CASS server and, at the database front-end AHDB, for each of the participating airlines. Additional traffic would be managed at ARINC by adding more load-sharing servers and Internet access circuits to the ARINC Operations Center Server Farm.

The CASS request and response are not large messages compared to most of the data that is transferred over the Internet for Web-based applications. The request averages about 200 bytes and the response averages 20 kilobytes—the average time for a request/response is 5 seconds. A maximum of 20 seconds required response time could cause some problems if the system grew to include several hundred airports, but this could be minimized during growth of the system by including compression technology. The ARINC CASS system averaged 3,500 requests per day in February 2007.

Feasibility

The CASS System is in use at most major airports. The primary requirement to take advantage of this system for security screening is a PC with Internet access. In the CrewPASS concept, ARINC would provide a web-based application that a TSA screening agent would use to issue an access request for the airline crew member. Operation of the CrewPASS prototype would mirror the operation of CASS, whereby the airline employee would provide the TSA screening agent with the prerequisite identification card, and the agent would generate an electronic message requesting access to the secure area of the airport. The request would be forwarded to the ARINC CASS server, which would route the query to the airline's designated database. The approval or denial response would be routed back through the ARINC CASS server, which would return the response to the TSA screening agent's computer terminal.

Discussion and planning could help define procedures most likely to improve throughput for crew members, without compromising security. This prototype could be demonstrated at a small number of locations for proof of concept with minimal investment in development and equipment. Continental Airlines has volunteered to help with prototype testing.



CrewPASS would immediately take advantage of the ongoing security background screening procedures in place for each airline as mandated by FAA and TSA directives and policy.

Costs

CrewPASS would immediately take advantage of the ongoing security background screening procedures in place for each airline as mandated by FAA and TSA directives and policy. Specific costs for these items would depend on the actual requirements mandated by the TSA. As proposed in this document, the incremental costs to the airlines and the TSA would be minimized.

Cost considerations would include the following:

- The TSA would require PC(s) with Internet connectivity. This equipment may be accessible already, shared, or need to be acquired.
- The TSA would require agent training that ARINC could provide at a per session cost to be determined based upon location.

- Developing a TSA-specific AHRS Web-based application to provide access request to ARINC server would require a one-time startup cost, which would be based upon actual changes required by the TSA.
- ARINC server access costs would rise because of increased message load. Message load would increase incrementally with each additional airport supported. Current ARINC pricing for CASS is $600/month/airline. ARINC is currently analyzing a price model to extend pricing to the TSA at a similar cost/month/airport basis.

Wireless PDA technology could also be used to improve the portability of the solution.

- Airline AHDB applications could be used at no additional costs to the TSA by using current CASS protocols to support a proof-of-concept test at selected airports.
- Airline IP circuits might need to be increased to support additional message load.
- Actual costs for screening airline pilots would decrease because of the significantly shorter time needed for CrewPASS screening versus physical screening.

Adding Other Airline Employees to CrewPASS

CASS was specified and implemented specifically to support secure access to the cockpit by airline pilots. CrewPASS could be implemented to identify other airline employees to further enhance security in conjunction with additional security measures as shown in Table 1. The implementation for most airlines would provide access to a more inclusive database that could include those employees, and a message could be generated that would confirm them as current employees in good standing. This method would prevent a suspended or fired employee from gaining access to the secure areas of the airport with an expired ID card.

Growth Versions of CrewPASS

CASS is implemented using open systems that are extensible and familiar to IT departments throughout the aviation community. The messages that are sent as part of CASS are based upon XML. The formats of these messages allow additional fields to be added when additional functionality is required. This will allow the addition of fields indicating roles or any other identification deemed relevant to this expansion of the system.

Future enhancements may require adding card readers to eliminate data entry at the security screening line. Because airlines do not issue a standard identification card to their employees, options include adding UPC stickers that may be optically scanned, or a separate credential such as a smartcard or magnetic strip card. In any case, the considerations for additional technology would be:

- assuring low cost of issuance,
- using COTS software and form factors to reduce cost of issuance,
- assuring durability, and
- maintaining an option for manual data entry.

Wireless PDA technology could also be used to improve the portability of the solution. The considerations mentioned above would still apply.

VI. Operational Considerations

A number of operational considerations must be addressed in the prototype phase of implementing CrewPASS, including the following:

- The location of CrewPASS monitors and/or other associated equipment would depend on the amount of space available at the installation site.
- The TSA must decide whether pilots or Transportation Security Officers would enter the data needed to make a CrewPASS request.
- Personnel who verify CrewPASS identification results would need minimal training. Crewmembers would be given similar training on how to use CrewPASS.

- CrewPASS should be tested at large, medium, and small airports during the prototype phase to ensure that all issues that may arise are adequately addressed. Areas at each airport that can be used to facilitate CrewPASS screening must be selected.
- The CrewPASS prototype should be used to determine whether the best data entry device is a keyboard, as is used for CASS, or some other type of device. An assessment of this issue should focus on ergonomics, speed, accuracy, and ease of use.

With a biometric-based screening system, TSA security equipment and personnel currently used at dedicated crew screening portals could be redeployed for passenger screening purposes.

VII. CrewPASS Benefits

Use of a biometric-based system to identify and screen pilots would reduce the TSA's airport screening staffing requirements and increase the screeners' operational efficiency. Considering the significant number of pilots traversing checkpoints on a daily basis, reduction or removing of flightcrew member traffic through checkpoint portals would position TSA screeners to better focus technological and human resources on the unknown commodities presented by the traveling public. The TSA's ongoing random employee screening would add another layer of security to CrewPASS.

With a biometric-based screening system, TSA security equipment and personnel currently used at dedicated crew screening portals could be redeployed for passenger screening purposes.

Airports and airlines would derive the customer service benefit of reduced waiting times at checkpoints. In addition, expedited passenger throughput would reduce the potential for a security event that might target or affect clogged checkpoint waiting lines. Airport operators would not be required to implement any new security technologies or alter their existing access control systems.

A wireless-based system could offer significant flexibility to airports and airlines in siting biometric-based access portals. They could be situated outside the view of the traveling public and away from crowded terminal areas. A portable system would offer flexibility to use airport areas that provide a convenient gateway for crew access to sterile areas. Because of the unique characteristics of individual airports, local challenges could more readily be addressed and resolved with the portability and simplicity of a biometric-based access system.

Personnel needed to operate the system would be supplied by the TSA. The simplicity of the system's design allows flexibility in this regard. The amount of training required for those operating the system would be minimal when compared to the training required of checkpoint screeners. The amount of training required for flightcrew members using the system would also be minimal.

Security Considerations

CrewPASS, a biometric-based crew identification system, would provide real-time verification of a pilot's identity and employment status,

two highly critical areas of concern. CrewPASS would virtually eliminate the possibility of a pilot-impostor with hostile intent entering the secured area, including the cockpit.

The system would also provide a more secure method of screening federal flight deck officers (FFDOs). CrewPASS would eliminate the need to follow, at passenger checkpoints, certain law enforcement protocols that make FFDOs readily identifiable by the public. Identification of FFDOs by the traveling public, and possibly by would-be terrorists, makes those pilots into targets because they are bringing firearms into the secure area of an airport. Another benefit of CrewPASS would be less likelihood that terrorists would identify a pilot as an FFDO and intentionally avoid flying on that pilot's airplane.

VIII. Recommendations

CrewPASS could bring several benefits:

. . . for the TSA—

- real-time verification of pilots' identification and employment status,
- a more secure method of screening FFDOs,
- elimination of the need to follow certain law enforcement protocols at passenger checkpoints,
- reduced airport screening staffing requirements,
- increased screener operational efficiency, and
- opportunities to redeploy TSA security equipment and personnel from dedicated crew screening portals to passenger screening;

. . . for passengers—

- reduced waiting times at security screening checkpoints;

. . . for airports and airlines—

- significant flexibility of wireless-based systems in siting biometric-based access portals;

. . . for flight crew members—

- less time spent in security screening, and
- less likelihood that screening would reveal FFDOs to terrorists.

ALPA therefore recommends that the TSA implement a prototype CrewPASS program and, after successful testing, deploy the system nationwide to electronically screen flightcrew members.

THIS DOCUMENT WAS PRODUCED BY AN OUTSIDE PARTY AND SUBMITTED TO THE OBAMA-BIDEN TRANSITION PROJECT.

APPENDIX 1

S.4

Improving America's Security Act of 2007
(Engrossed as Agreed to or Passed by Senate)

SEC. 1475. SECURITY CREDENTIALS FOR AIRLINE CREWS.

Within 180 days after the date of enactment of this Act, the Administrator of the Transportation Security Administration shall, after consultation with airline, airport, and flight crew representatives, transmit a report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation and Infrastructure on the status of its efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints. The Administrator shall include in the report recommendations on the feasibility of implementing the system for the domestic aviation industry beginning 1 year after the date on which the report is submitted. The Administrator shall begin full implementation of the system or method not later than 1 year after the date on which the Administrator transmits the report.

THIS DOCUMENT WAS PRODUCED BY AN OUTSIDE PARTY AND SUBMITTED TO THE OBAMA-BIDEN TRANSITION PROJECT.

APPENDIX 2

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

MAY 4 2006

Transportation Security Administration

Captain Duane E. Woerth
President
Air Line Pilots Association, International
1625 Massachusetts Avenue, NW
Washington, DC 20036

Dear Captain Woerth:

On behalf of Secretary Michael Chertoff, thank you for your letter of March 22, 2006, regarding the Transportation Worker Identification Credential (TWIC). We appreciate your offer to assist with swift implementation of TWIC.

TSA has ended prototype testing of TWIC and is working with the U.S. Coast Guard to publish a Notice of Proposed Rulemaking. Indeed, on April 25, 2006, Secretary Chertoff announced our intent to expedite the TWIC rulemaking. This rule and the subsequent final rule will implement the TWIC program for the maritime transportation mode. Implementation discussions for the aviation and surface modes will follow the initial TWIC rollout for the maritime mode. We recognize that flight crews travel through multiple locations on a daily basis and would benefit from being able to use a single identification credential such as TWIC. As we consider how best to leverage TWIC's capabilities in the unique airport security environment, we welcome your thoughts.

We look forward to making this vital national security program a reality. By utilizing technology and biometrics, TSA is working toward implementing a program that will allow a better means to identify workers requiring un-escorted access to secure areas. This will provide security managers another tool to ensure that the Nation's transportation systems and workers are secure. I have asked the General Manager for Commercial Airlines to keep you abreast of our progress as we move forward. I look forward to seeing you again.

Sincerely yours,

Kip

Kip Hawley
Assistant Secretary

Duane-
I will work on this to get pilots in a biometric program ASAP. Thanks for your help on this + everything else! - Kip

APPENDIX 3

TSA, AAAE, ACI-NA and NATA Announce Industry-Cooperative Employee Screening Plan

April 18, 2007

Media Contact:
TSA Public Affairs—(571) 227-2829

WASHINGTON—The Transportation Security Administration, American Association of Airport Executives (AAAE), Airports Council International–North America (ACI-NA) and National Air Transportation Association (NATA) today announced plans to measurably maximize the effectiveness of screening employees at airports. The six-point plan to harden and bolster employee screening utilizes a risk-based approach.

"Our strategy is to be nimble, flexible, mobile, and above all, dynamic," said TSA Administrator Kip Hawley. "Effective security requires partners working together within a network of overlapping measures around which terrorists cannot easily engineer. For that reason, we achieve a better overall security result by using our resources flexibly, not tied down at checkpoints checking and rechecking people that work at the airport every day."

Over the next 90 days, TSA, ACI-NA, AAAE and NATA, through a working group, will develop the standards and solidify the implementation timeline for the plan. The plan will include testing of six key measures, followed by a phased rollout to the 452 commercial U.S. airports.

The six key measures include:

1. **Behavioral recognition:** growing the population beyond TSA to include airport employees trained to recognize hostile intent.
2. **Employee training:** raising awareness of suspicious behavior and implementing incentives for reporting anomalies.
3. **Targeted physical inspection:** building upon TSA's random, unpredictable employee screening measures to include roving security patrols.
4. **Biometric access control:** expanding current use of fingerprint, iris, limited access and recorded access control measures.
5. **Certified employees:** creating a new level of employees that are subject to a more rigorous, initial level of scrutiny on a voluntary basis, allowing them to be removed from the regular, but not random, screening regimen.
6. **Technology deployment:** continuing to support the development of security technology including cameras and body imaging.

The collaborative employee screening plan builds upon the layered approach already in place at the nation's airports, which includes perpetual vetting of employees against watch lists, badge and keypad-protected entry points, and TSA employee screening patrols and surges.

"Airports must have a multi-layered security system for employees on the airside of airports precisely because it's an environment with many potentially dangerous 'things' including tools, fuel and other objects that are critical to normal airport operations," AAAE President Chip Barclay said. "Targeted, unpredictable physical screening is an important part of that system, but our top priority must be to eliminate dangerous people through strengthened vetting and background checks. We have to know the employees, improve background checks, and use targeted physical screening that isn't predictable if we want to effectively screen this critical population."

"Airports believe that the most effective security measures are 'risk-based,' focusing resources to provide the highest level of security," said Greg Principato, president of ACI-NA. "The six-point program being developed by airports and TSA will allow us to evaluate different combinations of programs and technologies. We can then implement

the measures which provide the greatest security benefits for airports and the traveling public."

"NATA's airline service companies and fixed-based operators recognize the importance of improving employee screening at America's commercial airports," NATA President James K. Coyne stated. "We believe that this new initiative will bring together the key stakeholders to address employee screening and provide effective solutions to ensure that America's commercial airports remain the safest in the world. NATA and its member companies look forward to participating in the development of these new voluntary measures over the next 90 days."

TSA Enhances Security With Employee Screening

Layers Of Security

While passengers around the nation are very familiar with the security checkpoint, they may not be as familiar with one of the newest enhancements to aviation security, roving patrols of Transportation Security Officers screening employees on the secure side of the airport.

The program, started last fall, deploys officers anywhere, anytime to inspect workers, their property and vehicles. These officers ensure workers follow proper access procedures when entering secure areas, display the appropriate credentials, and do not possess items unrelated to their work that may pose a security threat.

"Anyone accessing sterile and secure areas of the airport should expect that they could be screened at any time," said Earl Morris, TSA's Deputy Assistant Administrator for Security Operations. "This initiative is one more measure that adds to our strong, layered approach to aviation security."

Outside the airport, random inspections include scrutinizing delivery trucks or personal vehicles at access gates. Inside the airport, roving patrols screen workers with hand held metal detectors and examine property for threat items that are unrelated to their work. Temporary checkpoints are also created beyond access points to ensure access protocols are followed and workers are screened before entering the terminal. These measures do not impact wait times at security checkpoints.

Airport employees receive a security threat assessment prior to receiving credentials and access privileges. Security threat assessments consist of a criminal history records check and vetting against terrorist watch lists and are required for not only airport personnel but also individuals with access to public areas that possess airport credentials. This includes taxi drivers, parking lot attendants, vendors and shuttle bus drivers who have identification issued by the airport.

Airports are also required to develop Airport Security Plans that lay out physical security measures, procedures for safeguarding access control and other protocols specific to the facilities and area around an individual airport.

Individuals who violate security protocols may receive a civil penalty that varies depending on the action and circumstance.

APPENDIX 4

HR 1413:

Mrs. LOWEY (for herself, Mr. THOMPSON of Mississippi, Ms. GINNY BROWN-WAITE of Florida, Ms. JACKSON-LEE of Texas, and Mr. MARKEY) introduced the following bill; which was referred to the Committee on Homeland Security

---

A BILL

To direct the Assistant Secretary of Homeland Security (Transportation Security Administration) to address vulnerabilities in aviation security by carrying out a pilot program to screen airport workers with access to secure and sterile areas of airports.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. ENHANCED PERIMETER SECURITY AND ACCESS CONTROL THROUGH COMPREHENSIVE SCREENING OF AIRPORT WORKERS.

(A) Pilot Program—Not later than 120 days after the date of the enactment of this Act, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall carry out a pilot program at 5 service airports to screen all airport workers with access to secure and sterile areas of the airport in accordance with section 44903(h) of title 49, United States Code.

(B) Participating Airports—At least 2 of the airports participating in the pilot program shall be large hub airports (as defined in section 40102 of title 49, United States Code). Each of the remaining airports participating in the pilot program shall represent a different airport security risk category (as defined by the Assistant Secretary).

(C) Screening Standards—

(1) IN GENERAL—Except as provided under paragraph (2), screening for airport workers under the pilot program shall be conducted under the same standards as apply to passengers at airport security screening checkpoints and, at a minimum of 2 airports, shall be carried out by private screening companies that meet the standards in accordance with section 44920(d) of title 49, United States Code.

(2) DESIGNATED SCREENING LANE—In addition to the requirements under paragraph (1), each airport participating in the pilot program shall designate at least one screening lane at each airport security screening checkpoint to be used exclusively to screen airport workers under the pilot program.

(D) Vulnerability Assessments—As part of the pilot program under this section, the Assistant Secretary shall conduct a vulnerability assessment of each airport participating in the pilot program. Each such assessment shall include an assessment of vulnerabilities relating to access badge and uniform controls.

(E) Technology Assessments—Airport operators at each airport at which the pilot program under this section is implemented shall conduct an assessment of the screening technology being used at that airport and submit the results of the assessment to the Assistant Secretary. The Assistant Secretary shall compile the results of all the assessments and provide them to each airport participating in the pilot program.

(F) Duration—The pilot program shall be carried out for a period of not less than 180 days.

(G) Authorization of Appropriations—There are authorized to be appropriated such sums as may be necessary to carry out this section.

(H) Report—

(1) IN GENERAL—Not later than 90 days after the last day of the pilot program, the Assistant Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the results of the pilot program.

(2) CONTENTS OF REPORT—The report shall include the following:

(a) An assessment of the effect of screening all airport workers with access to secure and sterile airport areas on screening and logistical resources.

(b) An assessment of the security improvements that are achieved from screening such workers.

(c) An assessment of the costs of screening such workers.

(d) The results of the vulnerability assessments conducted under subsection (d).