

# Coalition of Airline Pilots Associations



## Pilot Biometric IDs

**Background:** CAPA's long-standing goal has been to both encourage and facilitate the implementation and standardization of high-level authentication methods to positively verify the identity of all individuals who are authorized flight deck access on both passenger and all-cargo carriers.

Currently, airline pilots are screened over 2,000,000 times each month by the TSA. The "Implementation of the Recommendations to the 9/11 Commission Act of Aug. 2007", provided legislative momentum with mandates to properly identify and expedite screening of crewmembers to meet an August 2010 program deadline. CAPA, SWAPA, SWA, Priva, TSA and BWI airport managers initiated "Secure Screen" as a joint 60-day pilot biometric ID test project. The Secure Screen "test" by all accounts from the TSA, vendor, airport managers and pilot participants was highly successful.

This year the Known Crewmember Program headed by the Air Transport Association (ATA) was approved for use by the Transportation Security Administration (TSA). The earlier addition known as CrewPASS was tested at three east coast airports. This enhanced process adds a level of security above what we have today, but it does not meet the securest standard: a real-time, verifiable biometric process.

We are 100% in support of the Known Crewmember Program which not only raises the security level from its current level, but builds the infrastructure necessary for the addition of the real-time, verifiable biometric process that CAPA seeks. The House Aviation Subcommittee is seeking a requirement for biometrics on pilot's licenses and we believe that working together with the Subcommittee would result in a solution that would provide safer, more secure access to aircraft.

### Primary Considerations:

- Counterfeiting of ID cards is acknowledged as a wide-spread nationwide security problem; There are numerous federal agencies whose officers are authorized to carry lethal weapons aboard commercial aircraft.
- Due to the limited design of the current airline/airport credentials, no one can positively authenticate the identity of any individual to prevent unauthorized flight deck access.

- Currently, airline pilots are screened over 2,000,000 times per month by the TSA which creates an undue burden on the crewmember and nearly 45,000 Transportation Security Officers.
- No single workable standard applied at the nation's airports to date.
- "Credentialing ID" cards contain only pictures and/or magnetic swipe cards that are easily counterfeited, lost or stolen which compromises the credential and may allow a fraudulent individual access to the aircraft flight deck.
- Extensive crewmember vetting with full background checks when coupled with biometric ID authentication would eliminate the need for 100% screening of crewmember's carry-on baggage.
- Canada currently uses airport employee and crewmember Biometric ID cards throughout the country for screening and access to sterile partitions of their airports.
- CAPA's passenger and all-cargo pilot members possess real-time operational experience and expertise in the aviation security arena and desire to be positive resources to the TSA to enhance the total security process.
- Include both passenger and all-cargo pilots in aviation biometric solution.

**CAPA Recommendations/Solutions:** CAPA supports the use of biometric technology in all personnel IDs to ensure the identity of airline industry employees with access to the aircraft or restricted ramp access.

- Issue crewmember "Biometric ID Credentials" for all part 121 and part 135 passenger and all-cargo pilots, aircraft mechanics, cabin crewmembers and any person with access to the flight deck as soon as feasible.
- Publish a date certain for implementation of this issuance.
- Expedited implementation of crewmember biometric ID credentials and associated changes to TSA screening protocols would *relieve the screening burden for more than 45,000 TSA Transportation Security Officers (screeners)*.
- "Random" full-screening protocols should also be retained.