

Statement of Carter Morris
Senior Vice President, Transportation Security Policy
American Association of Airport Executives
House Homeland Security Subcommittee on
Transportation Security and Infrastructure Protection
The Future of the Registered Traveler Program
September 30, 2009

On behalf of the American Association of Airport Executives (AAAE) and the thousands of men and women the Association represents who manage and operate primary, commercial service, reliever, and general aviation airports across the country, I want to thank the subcommittee for the opportunity to reflect on the future of Registered Traveler (RT). We remain grateful for your long-standing interest in and support for this important program.

The imperative to move forward with some sort of “trusted traveler” program will only increase as traffic begins to return to the aviation system, which most analysts agree will happen in the near future. Prior to the economic downturn, the situation at many airports was approaching unbearable with growing lines at screening checkpoints frustrating passengers and creating a dangerous safety and security situation. While the temporary downturn in traffic has pushed many of these problems to the back burner, there is little doubt that they will soon return – making it all the more important that we are here today discussing a concept that holds tremendous promise in enhancing security while improving efficiency in the airport environment.

I also want to take the opportunity to recognize and thank this subcommittee and the full committee for the provisions included in TSA reauthorization legislation – H.R. 2200 – aimed at fortifying the RT program and the trusted traveler concept. In our estimation, the approach you have taken as part of that legislation to enhance the background screening process for enrollees and to evaluate program improvements, including the possibility of expediting the screening process for program participants, are extremely helpful and important. We firmly believe that those changes can and should be integrated into risk-based aviation security operations at airports.

The changes you have advocated in H.R. 2200 would bring the program in line with what airports and our industry partners have recommended since the earliest days of discussion regarding the program. As you know, many of these key elements – including security threat assessments for enrollees and the utilization of technology to provide screening benefits for program participants – were present in the early days of the program. Unfortunately, these benefits eroded and disappeared over time, lessening the value of the program and its attractiveness to airports and the traveling public. The good news is that with many important pieces in place and with many lessons having already been learned, a successful trusted traveler program is well within our reach.

Airports Have Long Supported Trusted Traveler Concept and Development of RT

AAAE and the airport community have long supported the “trusted traveler” concept as an innovative security layer that focuses limited federal resources on the areas of greatest impact within the aviation system.

AAAE President Chip Barclay (along with Southwest Airlines executive Herb Kelleher and law enforcement veteran Ray Kelly) was a member of the high-level airport security Rapid Response Team created in the immediate aftermath of 9/11 by then-DOT Secretary Norman Mineta to deliver detailed recommendations for improving security within the national aviation system. In its report issued in

October 2001, the Rapid Response Team determined that “There is an urgent need to establish a nationwide program of voluntary pre-screening of passengers, together with the issuance of ‘smart’ credentials, to facilitate expedited processing of the vast majority of air travelers and to enable security professionals to focus their resources more effectively.”

The concept subsequently received the strong endorsement of the 9/11 Commission and has been advocated by numerous others. The trusted traveler concept allows for intense focus on individuals who, at no cost to government, voluntarily provide biographic and biometric information, freeing resources at screening checkpoints to focus on those for whom little is known. The result is enhanced security and improved efficiency at screening checkpoints.

Working closely with TSA, airports and the technology community; AAAE has taken a leadership role over the years in championing the concept and pursuing its nationwide implementation with the Registered Traveler (RT) program. Although not directly responsible for processing passengers at screening checkpoints, airports long ago recognized that there was great potential value in terms of enhanced security and efficiency with the deployment of a nationwide, interoperable RT program. Airports also understood that they were uniquely situated to bring interested parties together to chart a course that would result in the successful deployment and operation of the program.

In June 2005, AAAE – at the urging of several of our airport members – formed the Registered Traveler Interoperability Consortium (RTIC). The goal of the RTIC was to establish common business rules and technical standards to create a permanent, interoperable and vendor-neutral RT program. In addition to nearly 60 airports, RT service providers and leading biometric and identity management companies were active participants in the consensus-driven process as was the Transportation Security Administration, which played a critical role in establishing and ensuring compliance with stringent federal security standards. AAAE appeared before this subcommittee in November of 2005 to detail the work of the RTIC and airport efforts to pursue a nationwide, interoperable RT program.

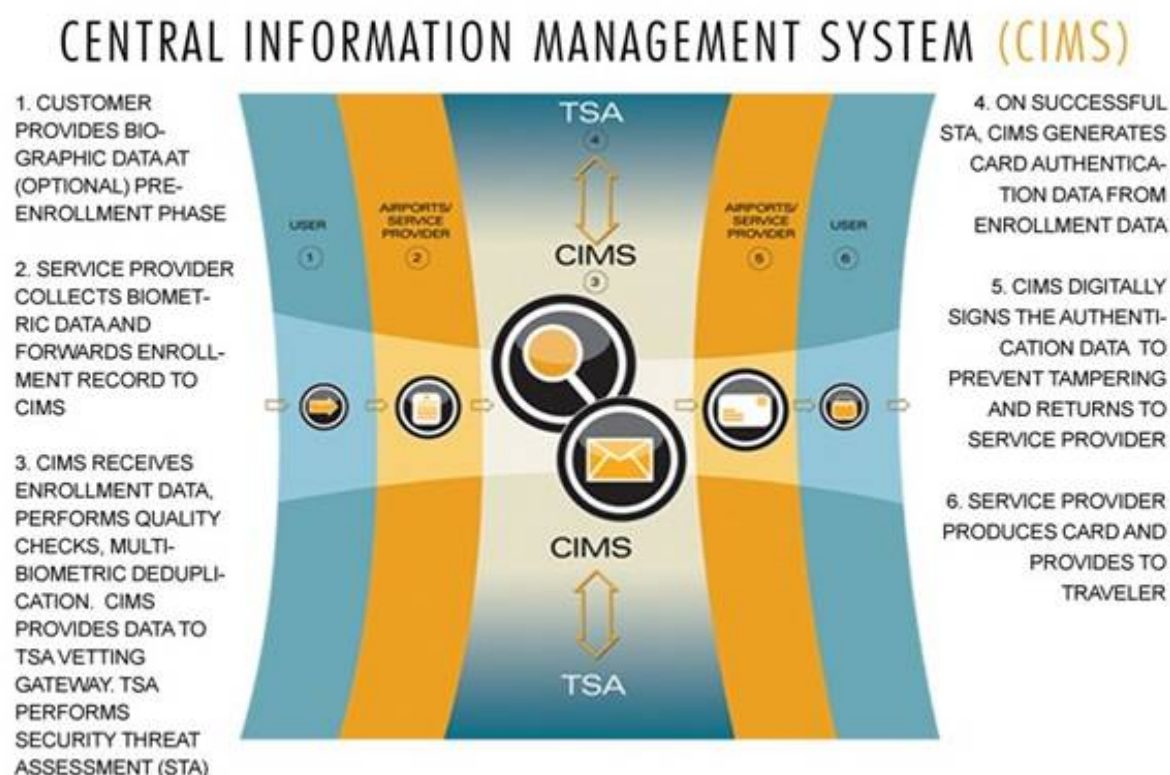
Throughout 2006, the RTIC worked aggressively to define, develop and implement the RT program at interested airports. In 2006 alone, the group dedicated more than 500 work hours to create the RTIC Technical Interoperability Specification, a detailed, 158 page technical standards document approved by the TSA that serves as the technical requirements for the interoperable RT program that eventually grew to more than 20 airports prior to the recent cessation of the program. The RTIC technical specification has been updated numerous times since it was first created and serves as a living document that can be altered to reflect future program requirements.

While there have certainly been challenges and frustrations along the way – many of which are being explored as part of this hearing – the experiences with the RTIC make clear that the best path forward for the RT program – or any subsequent trusted traveler concept – is one in which federal resources and standards are combined with the knowledge, expertise and creativity of airports, airlines, and aviation-oriented businesses. That approach led to the successful launch of RT as a secure, interoperable, nationwide program, and we remain convinced that the future of the program depends on effective partnerships between the federal government and the private sector.

The Central Identity Management System (CIMS) – Security and Interoperability

In addition to facilitating the development of the business rules and technical standards that proved critical to getting RT off the ground, AAAE’s owned and operated Transportation Security Clearinghouse developed and runs a TSA-certified and audited centralized identity management system known as the Central Information Management System or CIMS.

The CIMS is the world's most advanced interoperable information management system of travelers' biometric data. The first of its kind, CIMS enables verification of registered individuals with two types of biometrics by any certified operator at any participating airport with the very highest level of accuracy and security. As part of RT, the CIMS has been responsible for several key functions, including processing all records for program enrollees, interfacing with the TSA for background checks, ensuring an unbreakable chain of trust from vetted enrollments to issued credentials, to revoking credentials. Notably, the CIMS is capable of accommodating multiple biometrics, including fingerprints and iris.



The CIMS, which is capable of processing literally millions of enrollments from independent locations across the country, served as the critical engine that facilitated interoperability at various airport locations among multiple vendors. A key component of the RT program and of any trusted traveler program going forward is interoperability, meaning that participants who sign up in Phoenix must be recognized and accepted as they travel to other airports that have chosen to participate in the program, be it Denver, Atlanta, Washington or other airports throughout the aviation system. CIMS, through its standards-based and vendor-neutral architecture, provides the back-end security and technology that enables interoperability. As a result of the CIMS, the RT cards issued to over a quarter of a million participants in the RT program are among the most secure and interoperable non-federally issued credentials issued to the general public.

The CIMS was built with strict oversight from TSA and has been audited by the agency repeatedly to ensure full compliance with the broad array of federal security requirements pertaining to privacy and data protection, among others. Last year, the CIMS was recognized by the National Electronic Commerce Coordinating Council (eC3) as the 2008 Excellence Award winner for innovation in protecting the privacy and integrity of citizen information.

I would note that since the RT program ceased earlier this year, we have taken every precaution to continue to protect enrollee data in strict compliance with TSA requirements. We have been in constant contact with the agency and stand ready to comply with any future demands pertaining to such data.

We are proud of the CIMS and firmly believe that it holds tremendous value as part of RT or any future trusted traveler program. From a technical standpoint, the CIMS has proven itself invaluable, serving as the critical hub for facilitating interoperability among service providers and at airports across the country and for processing necessary checks and security controls. In its three years in operations, CIMS supported a system of four independent service providers at 22 airports with more than 250,000 actively enrolled participants. Whatever shape a future trusted traveler program may take, it is clear that the CIMS can and should continue to play a central role in performing key functions.

Airports Stand Ready to Support a Future Trusted Traveler Program

As is evident by today's hearing, there are a number of policy questions regarding the future of the program that must be answered by TSA in collaboration with the Congress. Among other things, policymakers must consider the specific role of TSA with the program, whether it will serve as a "front-of-the line" service or a security program with a resumption of security threat assessments or other checks, and whether or not program participants should be afforded screening benefits, such as leaving shoes on or laptops in their cases as they are processed through checkpoints.

While airports may have differing views on some of these key questions, there is broad agreement that any future trusted traveler program must function primarily to enhance security and expedite the travel experience. Those two pillars are the primary values that the nation's frequent air travelers want as well and that each of you as policymakers rightly will demand. By enhancing efficiency at airport screening checkpoints, TSA screeners will be able to better focus their limited resources on the critical task of providing more rigorous screening to individuals about whom we know less than those who have voluntarily submitted their background for extensive vetting and clearance.

The unique operational relationships between airports and TSA forged through this program can also serve as a platform for process and technology innovation at checkpoints. Emerging detection and surveillance technologies can be tested as a part of the trusted traveler process with less risk and more impact than with isolated pilot programs.

As each member of this subcommittee knows as a frequent traveler, every airport is unique. A successful, long-term trusted traveler program depends on the implementation of a technical, operational and business model capable of supporting individual airport needs, while providing the common infrastructure that allows passengers to use this capability at any airport nationwide. In recognition of that fact, it is critical that any future program continue to be airport-driven and run outside of government with careful and consistent government standards and oversight.

In terms of specifics, many of the initial principles outlined by airports and our partners working with the RTIC arguably remain as valid today as they did some three years ago. At that point, RTIC members agreed to support a system where:

- Qualified applicants in the RT Program will agree to voluntarily provide TSA- specified personal data, both biographic and biometric, which will be used by TSA to assess the security threat of each participant.
- Service providers will be responsible for enrollment operations, including collection and verification of personal data of eligible applicants. Service providers must protect and maintain all personal data

related to an applicant in a secure manner and prevent the unauthorized disclosure of the personal data.

- Service providers must securely transmit valid application enrollment data to the Central Identity Management System (CIMS). The CIMS will receive enrollment data from the RT service providers and will validate and perform duplicate checking of received enrollment data and forward data to the TSA for security threat assessments.
- The TSA will conduct the security threat assessments and return results daily.
- On receipt of notification of an acceptable security threat assessment for an applicant, the CIMS will notify the RT service provider for that applicant of the updated status of the applicant and will forward the applicant's credential information to the service provider.
- The credential information sent to the service provider will include a digitally signed biometric template generated by the CIMS which will ultimately be placed on RT participants' cards. The central issuance of the biometric template ensures technical interoperability but also importantly provides a chain of trust between an individual's biometric and the same individual's vetted identity.
- Service providers will issue and deliver participants' membership cards (e.g. smart cards). Service providers must notify CIMS of any future changes in the status of their participants, such as lost or stolen cards. Service providers are also responsible for customer service, including communicating with applicants regarding their approval status and responding to applicant and participant inquiries.
- Service providers may not unnecessarily disclose biographic and/or biometric data required for the purpose of the RT Program and collected by the service provider from RT Program applicants or participants. Service providers may not sell or disseminate any biographic and/or biometric data required for the RT Program and collected by the service provider from RT Program applicants or participants for any commercial purposes without the approval of the airport.
- Participating traveler processing will occur at the airport's security checkpoints. The placement of the RT screening stations will be located in front of the TSA passenger screening areas. Passengers that are not enrolled in the RT Program or are not approved when presented at the RT processing area will use the normal TSA security lines/lanes. Passengers that are enrolled and approved will use the designated RT security screening lines/lanes.
- Biometric technology will be used for traveler identity verification at the RT screening stations. Once a participant presents their membership card, fingerprint and iris biometric features will be used to verify passenger identity. Proposed biometric systems shall be currently operational, highly accurate, cost effective, and capable of confirming the identities of large populations within short time constraints.
- Service providers will operate the RT screening stations, including the timely update of system and card revocation status to ensure fast, secure and reliable verification and status-checking at the airport checkpoint.
- Service providers are responsible for installing, furnishing, integrating, operating and maintaining all of their required equipment and systems.
- The RTIC will create and maintain the technical and business rules for the RT Program. The RTIC will operate a certification program for RT service providers to validate the conformance of their

systems, service levels, and processes with the RT Program rules. Service providers will be required to undergo an annual re-certification and auditing of their systems and processes.

- Service providers will market the RT program to potential applicants and will use standardized RT Program logos and signage within their marketing.

While some adjustments to this model may be necessary and appropriate, it is clear that the basic framework outlined here offers a roadmap for a re-constituted program that offers great prospects for sustainability. We believe that these principles are in line with those outlined by the subcommittee in H.R. 2200.

In closing, I would emphasize the tremendous work that has been done to this point to get a viable, interoperable trusted traveler program off the ground with RT. With all of the pieces in place from a technical and business process standpoint, the only thing missing is clear direction and certainty as to what a future program may entail. The interest level of the traveling public will undoubtedly increase as traffic returns to our nation's airports as will the imperative to have a workable program in place.

AAAE and the airport community remain committed to working with our industry partners, with Congress, and with TSA to make the promise of a trusted traveler program a reality. Thank you very much for the opportunity to appear at this important hearing.