

**STATEMENT OF
JOHN SAMMON
ASSISTANT ADMINISTRATOR FOR TRANSPORTATION SECTOR NETWORK
MANAGEMENT**

**DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION**

**AT A HEARING ENTITLED
“THE FUTURE OF THE REGISTERED TRAVELER PROGRAM”**

**BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION SECURITY
AND INFRASTRUCTURE PROTECTION
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES**

SEPTEMBER 30, 2009

Good afternoon Chairwoman Jackson-Lee, Representative Dent, and distinguished members of the Subcommittee. It is my privilege to appear before you today to discuss the future of the Registered Traveler (RT) Program from the perspective of the Transportation Security Administration (TSA).

Registered Traveler: An Overview of the History

The Aviation and Transportation Security Act (ATSA) authorized TSA to “establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.”

Based on this legislative mandate, TSA undertook federally funded pilot programs to explore new technologies, the needs of passengers and stakeholders, and opportunities for private collaboration in order to develop a comprehensive RT program. During the summer of 2004, the Registered Traveler Pilot Program was initiated at five airports on a staggered basis around the country. In 2005, TSA initiated a new pilot, known as the Private Sector Known Traveler, at Orlando International Airport (MCO), to test the feasibility of a public-private partnership model for the RT program. Following the Orlando pilot, TSA worked with private industry to roll out an expanded public-private partnership pilot to test interoperability among multiple service providers. The RT Interoperability Pilot (RTIP) was a fee-funded program.

The prospect of a terrorist not identified on a watch-list raised questions about the viability of an RT program. This scenario was made abundantly clear in July 2005, when such terrorists attacked the London transit system. Accordingly, TSA decided to devote its resources to other security-focused initiatives. Given the public interest in the program, however, TSA decided to partner with private sector entrepreneurs, airlines, and airports to facilitate a market-driven RT program, provided such a program would not create any security risk to the system. This led to the formation of a private sector-led program announced in February 2006.

Private sector partners acted swiftly to move the program forward and established interoperability standards that were approved by TSA in May 2006 – giving RT and TSA access to an interoperable biometric credentialing system that had been constructed in less than a year.

Following the approval of standards, TSA developed a comprehensive set of guidance documents allowing the private sector to implement the interoperability pilot phase.

Implementation of the Registered Traveler Interoperability Pilot (RTIP) began with the release of the RTIP Fee Notice in the Federal Register. The initial fee of \$28 per participant covered TSA's costs for vetting and program management. Any additional services or costs associated with RTIP were established by the vendor, who, in turn, charged the participant for those services. This expanded pilot was designed to test the interoperability of biometric cards among multiple service providers at different airports across the country. Three RT vendors participated in the RTIP at approximately 23 airports.

After an evaluation of the results of the RTIP, TSA issued a Notice in the *Federal Register* on July 30, 2008, announcing the conclusion of the pilot. TSA determined that this private-sector program did not provide any additional level of security. TSA determined that the security threat assessments (STAs) were not a value-add to the security process and therefore, the \$28 fee to conduct them was not good stewardship of taxpayer dollars. As a result, TSA ceased conducting the (STAs) on RT participants, while enabling RT to continue as a private sector customer service program without the TSA fee or STA.

Registered Traveler: An Overview of the Current Status

By July 14, 2009, the three vendors participating in the pilot - Unisys Corporation/Fast Lane Option Corporation (FLO), Clear/Verified Identity Pass (VIP), and Vigilant Solutions – had ceased operations. This prompted the need for TSA to ensure the appropriate handling of participant information that RT vendors had collected and stored throughout the program's duration. Accordingly, TSA

instructed sponsoring airports and airlines – the entities with which TSA has a direct RT relationship – to ensure that RT equipment and customer information complied with the security and privacy requirements set forth in the TSA RT Standards for Security, Privacy, and Compliance guidance. In addition, during the course of the RTIP, TSA used two systems -- one managed directly by TSA for watch list checking and one operated by the American Association of Airport Executives (AAAE) under an Other Transaction Agreement (OTA) with TSA to support interoperability, containing personally identifiable information (PII). Since one system was directly managed by TSA and AAAE's system interfaced with TSA's system to submit information for STAs, TSA has been responsible for ensuring that these two systems operate in a secure manner consistent with the requirements of the Federal Information Security Management Act (FISMA). Among other things, FISMA requires agencies to secure information maintained in information technology (IT) systems. The data in the system owned and operated by TSA was deleted on August 1, 2009, consistent with the applicable records retention schedule approved by National Archives and Records Administration (NARA).

The other system (operated by the AAAE) is referred to as the Central Information Management System (CIMS). While TSA immediately ceased collecting information from program applicants at the conclusion of the pilot, TSA also provided a 12-month transition period to allow participants who enrolled immediately before TSA ended the pilot to continue to enjoy the benefit of using their card at all RT locations regardless of the vendor. The CIMS continued to facilitate this interoperability during this 12-month transition period. However, with the conclusion of the RTIP and the 12-month transition period, TSA is reviewing its legal

obligations, including those under the Privacy Act, FISMA, and the OTA with AAAE regarding the information contained within the CIMS system.

Registered Traveler: Looking Ahead

DHS will continue to encourage interested vendors to work directly with airports, airlines, and TSA to identify and implement worthwhile concepts that will provide registered travelers a benefit, while still maintaining both the level of security needed to ensure the safety of our transportation system, as well as the confidentiality of personally identifiable information. As with any transportation security program, TSA will maintain its regulatory oversight role for any such concepts adopted in the RT program.

Conclusion

Madam Chairwoman, thank you again for the opportunity to discuss the future of the RT program. We look forward to working with Congress and other stakeholders on the future of this program and other programs that will enhance security for the traveling public while improving the traveling experience. I would be pleased to respond to any questions.