Transportation Security Administration Transportation Workers Identification Credential (TWIC)

The Transportation Security Administration (TSA) is mandated by federal legislation to develop an identification system for individuals requiring access to secure areas of the nation's transportation system. The Transportation Worker Identification Credential (TWIC) is intended for each worker requiring unescorted physical or logical access to secure areas of the nation's transportation modes (maritime, aviation, transit, rail, and other surface modes).

The TWIC will allow implementation of a nationwide standard for secure identification of transportation workers and access control for transportation facilities. Current estimates are that 12 to 15 million workers will require the TWIC to gain access to secure transportation sites. Each individual enrolled in the TWIC system will be positively matched to his or her credential via a reference biometric (or multiple biometrics) and will have undergone a standard background check.

The program infrastructure carefully balances security, commerce, and privacy requirements. The TWIC threat mitigation goals are to:

- Uniformly and consistently ascertain identities.
- Uniformly and consistently match an individual to a valid credential and background check.
- Uniformly and consistently conduct access threat assessment.
- Provide a tamper-resistant credential.

The TWIC is to be universally recognized so that workers will not require redundant credentials or background investigations to enter multiple secured work sites and will allow facilities to better manage site access. Additionally, the credential will have the capability to be used within a facility to meet multiple levels of secure access requirements.

The TWIC system will contain sufficient technologies to be compatible with the Government Smart Card Interoperability Specification (GSC-IS) while maintaining access to and within local facilities. This will enable the TWIC to leverage existing access control system investments, rather than require replacement of these systems at considerable expense. Additionally, the TWIC system will serve as the standard platform for future technology purchases at transportation facilities.

The TWIC program conducted two regional multi-modal pilot projects. The Los Angeles/Long Beach and Philadelphia/Delaware River areas were the TWIC regional pilot sites based on the broad range of facility types (e.g., mode, size, infrastructure), organization structures, transportation mode inter-relationships, and policy issues in each region.

TSA completed a technology evaluation in late 2003 and determined that smart card technology is the most appropriate technology for TWIC's requirements, providing a commercially available, secure solution for both physical and logical access. TWIC program personnel is now planning a seven-month prototype phase which will begin in early 2004 and will introduce biometric identifiers and contactless technology. The prototype phase will include both pilot regions and add Florida airports and seaports.

This profile was developed by the Smart Card Alliance Secure Personal Identification Task for the report, "Secure ID Systems: Building a Chain of Trust," available at http://www.smartcardalliance.org/alliance_activities/secure_id_systems_report.cfm. Additional information about the TWIC program can be found at http://www.tsa.gov/public/display?theme=68. For more information about how smart cards are used for secure identification applications, visit the Alliance web site at http://www.smartcardalliance.org.