Transportation
Security
Administration

PRIVACY IMPACT ASSESSMENT

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROTOTYPE

Version 1.0

November 5, 2004

Contact Point:

Lisa S. Dean
Privacy Officer
Transportation Security Administration

Reviewing Official:

Nuala O'Connor Kelly
Chief Privacy Officer
U.S. Department of Homeland Security

- **Introduction**

Legislative Overview

The Aviation and Transportation Security Act (ATSA), Public Law (P.L.) 107-71, authorizes the Transportation Security Administration (TSA) to assess security threats to the transportation system and develop policies and programs to counter those threats, including background checks for transportation workers with unescorted access to secure areas (49 USC 114(f)). Section 102 of the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295, requires the completion of background checks and issuance of biometric transportation security cards for all maritime personnel requiring access to secured areas of vessels and facilities. Finally, section 1012 the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), P.L. 107-56, requires a security threat assessment on commercial drivers who transport hazardous materials.

In accordance with these legislative authorities, TSA established the Transportation Worker Identification Credential (TWIC) Program in December 2001. The Program's objective is to design and implement a standardized secure credential for the identification of transportation workers whose duties require unescorted physical access to secured areas of the nation's transportation system, or logical (i.e., cyber) access to computer-based information systems that relate to the security of the transportation system. TSA is beginning a volunteer Prototype demonstration[1] (hereafter referred to as "Prototype") to evaluate the use of this credential at designated locations throughout the transportation system.

Prototype will be conducted at 36 facilities representing various modes of the transportation system, including air, rail, maritime, and mass-transit. As part of enrollment for Prototype, transportation worker volunteers will submit their biographical information to undergo a name-based security threat assessment aimed at identifying persons who pose or are suspected of posing a security threat to the nation's transportation system. Additionally, volunteers will submit their biometric identifiers to assure they have not been previously enrolled in the TWIC system during Prototype. Further, the biometric information will be used to verify that the rightful cardholder is presenting the card. Prototype is expected to end during the first quarter of 2005.

This Privacy Impact Assessment (PIA), conducted pursuant to the E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB), is based on the current design of the program and the Privacy Act system of records notices, Transportation Security Threat Assessment System (DHS/TSA 002), and Transportation Workers Identification Credentialing System (DHS/TSA 012), that were published in the Federal

[1] The State of Florida requires by statute that individuals accessing Florida's active seaports undergo an annual criminal history records check. See Florida statute, Title 22, sections 311.12 and 311.125. Specifically, section 311.125(2)(b) sets forth certain minimum statewide seaport security standards, including a uniform Port Access Credential Card to authorize access to any restricted area. Florida statute 311.125 directs the Florida Department of Highway Safety and Motor Vehicles to (1) consult with TSA, and (2) conform to the TWIC Program design. Therefore, Florida's 14 deepwater ports volunteered to take part in the Prototype. The criminal history background check done at the Florida ports will be completed by Florida under its statutory authority.

Register on September 24, 2004.[2] During Prototype, TSA will be analyzing the efficacy and efficiency of the system as it is designed. TSA may make changes or enhancements to the system. As required, TSA will amend this PIA prior to implementing any material changes to the TWIC system. This PIA provides further detail about the collection of personally identifiable information for the purpose of issuing credentials and conducting the name-based security threat assessments mentioned above.

- **System Overview**

The TWIC Program was established in response to identity management threats and vulnerabilities identified in the transportation system, and in accordance with requirements of the ATSA, MTSA, and USA PATRIOT Act. Threat examples include the following:

- Inability to positively identify individuals who seek to gain unescorted access to secure areas of the transportation system;
- Inability to assess the threat posed to the transportation system by those who seek or have unescorted access to secure areas of the transportation system due to a lack of background information, or the lack of uniformly determined background information; and
- Inability to protect current worker credentials against fraud.

To mitigate the identified threats, the TWIC Program will establish an integrated, credential (i.e., card) -based, identity management system for all transportation workers requiring unescorted access to secure areas of the nation's transportation system.

The TWIC Program will ensure that the identity of each TWIC holder has been verified; that a threat assessment has been completed on that identity; and, that each credential issued is linked to the rightful holder through the use of biometric technology. Local transportation facilities may then choose to grant access to those persons who have been issued the TWIC. As a condition of participating in Prototype, facility operators must agree that workers will not be penalized or denied access to the facility for not volunteering to participate in Prototype.

In July 2003, TSA completed the TWIC technology evaluation to test and evaluate a range of card-based technologies in operational transportation facilities. As a result of this evaluation, it was determined that the Integrated Circuit Chip (ICC) smart card is the most appropriate technology for the TWIC Program as it provides physical access security and computer access capability. The TWIC Program is currently entering Prototype to test the use of this credential at designated locations.

This Prototype will begin during the fall of 2004; it will include a comprehensive card-based secure credentialing system, to include enrollment, threat assessment checks, biometric security, card production, and issuance. The identification security of the TWIC Program is designed to

[2] 69 Fed. Reg. 57349-52 (Sept.24, 2004).

establish a "chain of trust" that ties the individual to a security check, and then the card to the individual through the use of a biometric identifier. During Prototype, a name-based threat assessment will be performed that will compare a volunteer's biographical information against terrorist-related databases.

Prototype Overview

Prototype is a voluntary initiative designed to test and evaluate a comprehensive program. This initiative will take place at transportation facilities on the East and West Coast, and the State of Florida that are volunteering to allow TSA to use their facilities as test sites. The East Coast region locations include facilities in and around Camden, NJ; Wilmington, DE; and Philadelphia, PA and Long Island, NY. The West Coast region locations include facilities in and around the Los Angeles/Long Beach, CA area. Florida's 14 deepwater seaports have also volunteered to take part in Prototype per the requirements outlined in Florida statute, Title 22, sections 311.12 and 311.125.

During Prototype, several critical steps will be designed, executed, and evaluated: pre-enrollment and enrollment processes; name-based security threat assessment; identity verification, including biometrics and card issuance; and use of the TWIC as positive identification for access to secure areas of the participating transportation facilities. By testing the integration of these steps, TSA will be able to assess the system's performance before making a decision regarding how the program should be implemented following Prototype.

As part of Prototype, TSA contractors, known as TWIC "Trusted Agents" will enroll the transportation workers who volunteer to participate in Prototype. These TSA contractors—who by law and contract must protect personal information covered by the Privacy Act—will perform this role on behalf of the government during Prototype on the East and West Coasts. These contractors will be specially trained and certified to serve as TWIC Trusted Agents in this capacity. In the State of Florida, employees of participating port facilities, and in accordance with Florida statute, will perform enrollment operations in addition to TSA contractors.

- **Collection and Use of Information**

What information is being collected and used for the security threat assessment and issuance of a TWIC in Prototype?

The TWIC Prototype is a strictly voluntary program for the participating transportation facilities, and for the transportation workers who volunteer to apply and submit biographical information to receive a TWIC. Workers at these facilities may choose not to participate. As stated previously, in fact, as a condition of participation in Prototype, all facility operators must agree individuals will not be penalized or denied access to the facility for not volunteering to participate. Those individuals who volunteer to participate in Prototype must provide the following information: complete name; address; phone number; Social Security Number; date of

birth; place of birth; employer and/or sponsoring organization and affiliation; biometric samples (fingerprint and/or iris scan); electronic signature, and digital photograph.

Additionally, participants must provide appropriate identity verification documentation, such as a birth certificate, driver's license, government photo identification, or similar document. The identity documentation verification process for Prototype will follow the Employment Eligibility Verification (Department of Justice Standard Form I-9) process commonly used by the federal government and commercial industry in the hiring process. The Department of Justice Standard Form I-9 is included as Attachment A of this PIA.

Why is the information being collected and who is affected by the collection of this data?

The personal information collected during Prototype will be used to establish the individual's identity, conduct a security threat assessment, and issue a credential. A TWIC will only be issued upon successful completion of: 1) the enrollment process, 2) a name-based security threat assessment, and 3) a biometric search of existing TWIC Prototype enrollment records. All Prototype volunteers are affected by this collection.

What information technology system(s) will be used for this program and how will they be integrated into a step-by-step process.

The TWIC Prototype system is composed of the following steps: employer/sponsor registration, participant pre-enrollment, participant enrollment, card issuance, and card revocation. These steps will occur in five possible locations: pre-enrollment through kiosks and web portals; the local enrollment centers; the TWIC Identity Management System (IDMS)[3]; the federal card production facility; and the TWIC local node[4] at the local facility. A description of the Prototype is set forth below. System details that ensure the secure handling and transmission of information to prevent unauthorized use are addressed in a later section of this PIA.

Employer Registration and Sponsorship

Every volunteer applicant will require sponsorship as part of the TWIC pre-enrollment process. The sponsor will be either the volunteer's employer, or, in the case of self-employed workers (e.g., self-employed truck drivers), a participating facility operator. In any case, sponsors must register the volunteer applicants before the applicant can apply (i.e., pre-enroll) for a TWIC.

[3]Also referred to as the TWIC database, IDMS will serve as a data repository, containing biographical data, photo images and biometric identifiers of TWIC applicants and holders.

[4] The TWIC local node is a TSA-owned and controlled computer or device that is installed at the local facility for purpose of biometric identity verification and communication with the TWIC database (i.e., IDMS). The local node itself does not contain any biographical or biometric information. The local node simply acts as a device to enable the local facility to connect to IDMS containing the biographical and biometric data. The node does not retrieve any information. It simply informs the facility operator of verification of identity.

Employers must register and establish a link between them and the volunteer applicants they wish to sponsor. The TSA contractor at participating Prototype locations will provide employers and other sponsors with instructions on how to register and sponsor volunteer applications.

During Prototype, employer registration will occur electronically via a secure web portal established by TSA. Employer registration will require the employer or facility operator to provide the following information, company name, address, type of business, and the company's Employer Identification Number (EIN)[5]. Once the registration form has been completed and submitted, TSA will begin the process for approving the entity as a sponsor. This process includes: (a) TSA confirmation that the employer or facility operator is a recognized business entity authorized to participate in Prototype; (b) documentation in IDMS that the entity has been approved by TSA to sponsor TWIC volunteer applicants; and (c) notification from TSA to the approved entities that they may sponsor volunteer applicants. Employers will then provide a list of employees they are sponsoring at the commencement of Prototype and may continue to do so throughout the test period.

Pre-enrollment

All TWIC applicants will pre-enroll as the first step of the enrollment process. The objectives of the pre-enrollment process are to facilitate submission of a complete enrollment application, and open an enrollment record in IDMS. Pre-enrollment may be conducted either remotely via a secure web portal, kiosk, paper application, or in-person at the enrollment center.

As stated previously, volunteer workers can begin the pre-enrollment process once they establish that they have a sponsor. The applicant will complete and submit to TSA the enrollment application with the required biographical information. Upon submission of the data, TSA will create an enrollment record that stores biographical data elements from the application. If a volunteer applicant does not want to provide some or all of the requested information, the volunteer will not be able to participate in Prototype. Upon generation of an enrollment record, the applicant will receive: (1) e-mail verification that the pre-enrollment process is complete, and (2) information regarding how to make an in-person appointment for enrollment.

Enrollment

Enrollment is the process of completing the application process and collecting biometric information. Biographical information may be provided during pre-enrollment. Any biographical information that is not collected during pre-enrollment will be collected during the enrollment process. Additionally, biometric information collection and identity verification that need to occur in person will be conducted during this process. During Prototype, enrollment will occur in participating transportation facilities[6].

[5] Also known as a Federal Tax Identification Number, an EIN is a nine-digit number that the IRS assigns to business entities. The IRS uses this number to identify taxpayers that are required to file various business tax returns.

As mentioned previously, a TSA contractor will perform the enrollment process by completing the electronic application that was initiated during the previous pre-enrollment process. Any application initiated in paper format will be converted to electronic form and securely stored in IDMS.[7] The TSA contractor will verify the applicant's information and collect the applicant's biometric samples, electronic signature, and digital photograph. Additionally, the volunteer applicant will submit original claimed identity[8] documents, which will be verified and/or copied into the enrollment record. All documents provided by the applicant will be immediately returned once copied or visually verified as authentic.

As discussed above, the identity document verification process for Prototype will follow federal standards, based on the Employment Eligibility Verification or I-9 process commonly used by the federal government and commercial industry in the hiring process. TSA contractors performing enrollment duties are required by law and contract to protect personal information in accordance with the Privacy Act and TSA privacy policies. Once collection is complete, all applicant enrollment information is encrypted and then securely transmitted to IDMS.

By design, and for security and privacy reasons, no enrollment data is stored at or by the local facility level. The enrollment record can only be viewed or retrieved by TSA or a TSA contractor who is certified to perform enrollment activities. The ability to retrieve or view an applicant's enrollment record is controlled by access controls including user authentication, which ensures only those with a need to access the data and proper training can retrieve or view enrollment information. In addition to this access control, physical privacy protections will be used. These physical protections include the use of "Privacy Screens" that prevent passers-by from viewing enrollment record information that may be displayed on the enrollment center workstation. Additionally, the enrollment center's physical security controls will be enforced to ensure that only TSA employees or TSA contractors with a need for access can enter the enrollment center and view personal information displayed on screens.

IDMS will be designed, developed, and operated by TSA, but physically located in a federally controlled Sensitive Compartmented Information Facility (or SCIF) with state-of-the-art secure network technology and physical security. SCIFs are certified and accredited to store, handle and process classified information. Although IDMS will not process classified information, the

[6] As noted previously, the process for Florida participants will differ as a result of the implementation of the State law. For example, in Florida and for all applicants governed by Florida statute, the Florida Department of Highway Safety and Motor Vehicles (DHSMV), through the Florida Department of Law Enforcement (FDLE), will permit only those applicants who have successfully completed the state required criminal history check apply for a TWIC. This "front-end" processing will be completed before the Prototype enrollment process can begin.

[7] The TWIC Program does not currently have a records retention schedule'; therefore, TSA will not dispose of paper applications collected during Prototype. TSA is working to develop a retention schedule for this program with the National Archives and Records Administration.

[8] These documents are also referred to as "breeder" documents.

system will benefit from the heightened security controls required to process classified data within this secure facility.

IDMS stores volunteer applicants' enrollment records. An enrollment record is composed of three components of information: biometric images, biometric templates and personally identifiable information. All enrollment record information will be stored in an encrypted format. As an additional layer of protection, IDMS will store each of these three information components separately (i.e., segmented) to prevent the entire enrollment record from being compromised. In any case, access to any of the three information components, individually or collectively, would yield only useless, unintelligible information since it is encrypted. Access to the entire enrollment record will be limited to those with an operational need to access the information.

When a volunteer comes to an enrollment center to complete the application process he or she will be asked to provide biometric data. The data will be collected for two purposes. First, biometric data is collected for identity verification purposes, i.e., verify that the biometrics of the person presenting the card match the biometrics information contained on the card. This is known as "one-to-one identity verification." Second, the biometric data is collected to run against biometric data contained in IDMS to determine if a volunteer applicant has previously attempted to enroll in Prototype. This is known as a "one-to-many" search.

As part of the Prototype enrollment process, ten fingerprint images will be collected and securely stored in IDMS. IDMS will convert all ten-fingerprint images to templates[9] extracted from the image so they can be safely used for biometric searches and matching. Two index finger templates will be included in the applicant's enrollment record.[10] These two templates will be securely loaded onto the card's integrated circuit chip during card production. The stored templates on the card will be used to facilitate "one-to-one" identity verification. This capability assures that the bearer of the card is the rightful cardholder. These fingerprint templates will also be maintained in IDMS to serve the "one-to-many" biometric search requirement. This capability prevents duplicate, fraudulent, or erroneous enrollments. During Prototype, TSA will collect an iris biometric sample at one location on the West Coast and one location on the East Coast. The purpose of collecting the iris biometric in addition to the fingerprint is to evaluate its potential use for identity verification in full-scale implementation of the TWIC system. In order to collect the iris sample, the applicant's iris will be imaged and converted to a template to conduct identity verification when the TWIC holder presents his or her TWIC to access secured areas of transportation facilities, as is the case with the fingerprint-based biometric. In all cases, IDMS will contain fingerprint templates for the purpose of conducting the "one-to-many" search to prevent alias or duplicate enrollment.

[9] The biometric template is a binary file created by processing the biometric images through a mathematical algorithm. This process cannot be reversed to recreate the biometric image from the template, and is therefore, secure.

[10] The remaining fingerprint images will be stored for use in the event a new template must be created.

Security Threat Assessment

As noted above, TSA will conduct a name-based security threat assessment aimed at identifying terrorist threats on volunteer applicants prior to issuing a TWIC. The biographical information collected from volunteer applicants during pre-enrollment and enrollment will be formatted and sent via secure password protected e-mail to TSA employees to run through terrorist-related databases that TSA maintains or uses. Any individual who meets the minimum criteria established by TSA as a possible match will undergo further analysis and screening. This involves an extensive review by agency personnel. Based on this further analysis and screening, TSA will then determine whether or not the individual poses or is suspected of posing a security threat.[11] A determination that someone poses or is suspected of posing a security threat is only made after a review by the Director of the Credentialing Program Office (CPO) who conducts the final review. The purpose of this process is to protect applicants from being incorrectly identified as a threat and to minimize the number of "false positives."

After this review, the name of any TWIC applicant posing or suspected of posing a security threat will be forwarded to the appropriate law enforcement and/or intelligence agency. TSA will continue this process by conducting security threat assessments on individual's issued TWIC cards during Prototype on an as needed basis for security purposes.

Card Production and Personalization

Once the threat assessments are completed for volunteers who have successfully completed the security threat assessment, the enrollment data is placed into a card format for card production. Then the information is encrypted and transmitted to a secure DHS federal card production facility that operates in accordance with an executed Interagency Agreement with TSA.

The card production facility will conduct an electronic quality control check on the enrollment record to ensure it arrived from an authorized enrollment center, an authorized user, and that the enrollment record was not modified or compromised in transmission. If the enrollment record was received intact, an electronic acknowledgement of receipt will be sent to IDMS, and used to update the enrollment record to reflect the current status of the enrollment record (i.e., receipt at card production facility). If the enrollment record does not pass the technical quality control check upon receipt at the card production facility, the applicant's enrollment record will be rejected, IDMS will be notified, and the originating enrollment center will be electronically notified of the anomaly for resolution. In the unlikely event of this occurring, IDMS will re-send the completed enrollment record to the central card production facility and the applicant's enrollment record will be updated to reflect the anomaly and the fact that the enrollment record was retransmitted. The resolution of this situation will not affect the applicant.

The information to be printed on the TWIC will be the applicant's name and photograph. Other information will be securely stored on the card's integrated circuit chip (ICC) for identity verification purposes. The information stored on the card will include biometric templates;

[11] During Prototype, TSA will not disqualify an applicant from being issued a TWIC based on criminal history.

name; biometric samples (e.g., fingerprint or iris scan); digital photograph; unique card serial number, and unique card number for the cardholder. The biographical information is electronically copied between the card's surface during printing and the ICC to enhance the chain of trust (i.e., the link) between the chip, the card and the individual. That is, the TWIC system will compare printed and electronic information to ensure that all elements match before the credential is deemed valid.

Once the applicant's TWIC is produced, it undergoes a card quality assurance check at the card production facility to ensure that all technologies and card security features work properly. If the card does not pass the quality control check, it will be physically destroyed in a secure and auditable process by the card production facility and the data will be re-entered into the card production process until the final product passes quality control standards. If the card passes the quality control check, the card's ICC is electronically "locked" to prevent any information from being disclosed without it first being "unlocked" by the individual volunteers in combination with the TWIC Trusted Agent at the enrollment facility.

Once the card is electronically locked, it will be ready for shipment, but it is not yet activated for access to secure areas. The electronically locked card is securely shipped by the production facility, via traceable means, to the originating enrollment center for issuance to the volunteer applicant. IDMS is notified electronically by the card production facility that the card has been completed and shipped, and the enrollment record is updated to reflect the most current status of the enrollment record. At this point, the applicant's electronic enrollment record at the central card production facility is destroyed. The card production facility's information security and inventory control procedures provide for the destruction and auditing of physical goods and logical data records upon completion of manufacturing credentials. The card production facility does not retain any personal records; thus, the typical risks of physical security are mitigated by the fact that enrollment information will not be retained at the facility.

Once IDMS receives the "card complete" notice from the card production facility, the enrollment record is updated to reflect the most current status. Once the card is received at the local facility enrollment center, the applicant is scheduled and notified to report to the enrollment center through the means requested by the applicant during enrollment. The notification methods may include electronic mail or phone call.

Issuance

Issuance begins when the applicant arrives at the designated enrollment center. In the presence of a TWIC Trusted Agent, the individual performs a biometric verification with the index fingers to verify identity, unlock and activate the TWIC, and complete the issuance process. This personal protection mechanism for activation (i.e., biometrics) provides much stronger security assurances than typical protections such as Personal Identification Numbers (PINs) or passwords. Once the transportation worker has been issued a TWIC, IDMS is updated to reflect that the credential has been issued. As previously mentioned, the issued TWIC cannot be used for access to secure areas until activated at the participating location, by the local facility operator. Once

the cardholder is in possession of his/her TWIC, the cardholder's next step is to request access to a participating local facility.

Privilege Granting

When a TWIC cardholder needs to gain local access privileges with an issued TWIC, the local facility will use the local TWIC node (a computer owned and maintained by TSA) connected directly to IDMS through a secure web portal. Access privileges are granted upon: (1) confirmation that the issued TWIC is still a valid card by checking the card's unique serial number in IDMS, and (2) verification of the identity of the person holding the card by using the biometric template stored on the card to match the cardholder's index finger. As a result, IDMS is notified that the local facility has granted the TWIC card holder local access privileges. The local TWIC node does not store any biographical or biometric information and simply acts as a tool to exchange information between itself and IDMS.

Facility administrators responsible for area security and their respective local access control systems can use the Card Holder Unique ID (CHUID), hereinafter called the unique card number, for managing unescorted access to secure areas. Local access control is granted or denied by comparing card numbers registered in the local access control system against the one presented by the cardholder at the time of attempting access. If the card presented to the electronic reader at the local facility is registered in the local access control system, then access is granted. If the card number is not matched, then the cardholder must contact the facility operator for resolution.

Although the TWIC card verifies that the holder is not a security risk, local facilities, not TSA, have full control over who has authorized access to their secure areas. Local facilities retain authority to grant or deny access to: (1) employees, and (2) people who require access to the facility to conduct legitimate business.

Revocation

Revocation of the card may be necessary for a variety of reasons, such as a lost, stolen, deactivated, or otherwise unusable card. Revocation may occur by "hot-listing" the card using the card's unique serial number. "Hot-listing" is a term of art used to describe cards that should not be used (i.e., honored) for unescorted access to secure areas. If the card is determined to be invalid, the cardholder must report to the enrollment center for resolution, and/or re-issuance of a new card.

What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?

Because Prototype is a voluntary phase of the TWIC Program, consent is a prerequisite for participation at the East and West Coast facilities.[12] Port participants in the State of Florida will participate after passing a criminal records history check, required under Florida law. In all cases, TWIC volunteer applicants will be provided a notice required by the Privacy Act, 5 USC 552(a)(e)(3). The notice will state the reasons for the collection of information, the consequences of failing to provide the requested information, and explain how the information will be used. Individuals who choose not to volunteer will continue to undergo the normal access procedures to the facilities they currently access.

The collection, maintenance, and disclosure of information will be in compliance with the Privacy Act and the published SORN for the Transportation Security Threat Assessment System "T-STAS" (DHS/TSA 002) and the Transportation Worker Identification Credentialing (TWIC) System (DHS/TSA012). Information about volunteers will be shared with TSA employees and its contractors who have a "need to know" for implementation of the TWIC Prototype. TSA contractors are contractually obligated to comply with the Privacy Act in the handling, use and dissemination of all personal information. As stated earlier, if TSA determines during the name-based threat assessment that an applicant may pose or is suspected of posing a security threat, TSA will notify the appropriate law enforcement and/or intelligence agencies.

Volunteer applicants will also participate in an electronic signature process conforming to the Electronic Signature (ESIGN) Act. This process will confirm presentation of and agreement with the above notices; confirm the intent to participate in the process; submit to a named-based threat assessment; and in the case of Florida, acknowledge the necessity of a criminal records background investigation.

Does this program create a new system of records under the Privacy Act?

No. This program is covered under two Privacy Act systems of records: Transportation Security Threat Assessment System (DHS/TSA 002), and Transportation Workers Identification Credentialing System (DHS/TSA 012), that were published in the Federal Register on September 24, 2004.[13] The purpose of these systems of records is to facilitate the performance of security threat assessments and the other key components of Prototype, and ensure transportation security throughout the duration of Prototype.

What is the intended use of the information?

The information is being collected and used during Prototype to confirm and establish an applicant's identity in the TWIC system, perform a security threat assessment, and issue a

[13] 69 Federal Register 57348-57352, September 24, 2004

personalized TWIC. The TWIC will be used during Prototype to allow participants unescorted access to secured areas in the participating regional facilities.

With whom will the information be shared?

The information will be shared with the appropriate TSA employees and TSA contractors involved in the design and development and implementation of Prototype who, by law and contract, are bound by the Privacy Act. During the enrollment process, a TSA contractor, who is also bound by law and contract to abide by the Privacy Act, and who will have been specifically granted access by the TSA program office in charge of Prototype, will review, enter, and authenticate an applicant's biographical and biometric information. TSA Contractors perform this function only after successfully completing training and certification for their position. Once the credential is issued to the authorized cardholder, the TSA Contractor within the enrollment center has no further interaction with the card or cardholder, until such time as issuance of a new or replacement card would be required, or in response to a cardholder's request to correct information previously provided by the cardholder during enrollment.

In accordance with Florida statute, those applicants who are governed by Florida statute will have their enrollment data shared with the DHSMV who will be executing and administering TWIC enrollment center activities. DHSMV will share the information with the FDLE, which will conduct the fingerprint-based full criminal history records check that is required under Florida law.

If a security threat assessment identifies an applicant who poses or is suspected of posing a security threat, TSA will notify the appropriate law enforcement and/or intelligence agency for further investigation. Sponsors will be notified of eligibility or ineligibility of a volunteer. The collection, maintenance, and disclosure of information will be in compliance with the Privacy Act and the published system of records notices.

How will the information be secured against unauthorized use?

All DHS/TSA and assigned contractor staff will receive appropriate privacy and security training, and have any necessary background investigations and/or security clearances for access to sensitive, privacy or classified information or secured facilities. TSA ensures this through legal agreements with its contractors and internal privacy policy enforcement with all DHS entities involved in processing the security threat assessments.

TSA's Privacy Officer is responsible for ensuring that the privacy of all volunteers is respected and for responding to individual concerns about the collection and retention of personal information during Prototype. The TSA Privacy Officer will review privacy issues related to this program to ensure that privacy concerns are considered in all aspects of this program. Additionally, TSA Integrated Project Team (IPT) Managers will be responsible for identifying and resolving any privacy-related issues and informing the TSA Privacy Officer of these issues.

The Chief Privacy Officer for the DHS will also exercise program oversight to ensure that privacy protections are integrated into the program and privacy issues are addressed promptly.

All data exchange will take place over encrypted data communication networks that are designed and managed specifically to meet the needs of Prototype. Private networks and or encryption technologies will be used during the transfer of information to ensure that Internet "eavesdropping" is not allowed and that data is sent only to its intended destination and to an authorized user, by an authorized user. Enrollment data may be temporarily stored at the TWIC enrollment centers for encrypted batch transmission to IDMS. As stated previously, a federally controlled Sensitive Compartmented Information Facility (or SCIF) will host IDMS with secure, state-of-the-art network technology and physical security.

IDMS is a data repository, containing biographical data, photo images and biometric identifiers. By definition this creates a general privacy risk. This risk is mitigated, however, by adhering to the guidance contained in the Privacy Act, which protects personal information from unlawful disclosure and the implementation guidance in section 208 of the E-Government Act, which requires this PIA. As a result, TSA has designed and developed IDMS and Prototype to mitigate the potential for privacy risk. Throughout the system requirements, appropriate processes for encryption and handling of data "at rest" and during transmission are followed to safeguard data confidentiality, integrity, and availability.

Biometric image data collected at the TWIC enrollment centers will be handled as sensitive personal information throughout the process. Biometric images will be stored as compressed and encrypted data, completely disassociated from personally identifiable information. IDMS will generate an "index key" that will serve as the only link between an enrolled individual's biographical information and biometric image data. In addition, biometric images and the biometric templates created from this data will be suitably handled to prevent any interception, alteration, release, or other data compromise that could result in unauthorized use. Biometric protection techniques outlined in International Committee for Information Technology Standards (INCITS) - 383 will be used to secure these biometric templates. Under no circumstances will any biometric data be retained in the local enrollment station after transmission to IDMS has been completed. Enrollment centers do not retain any information. System design and architecture will support the automatic deletion of any and all collected information (e.g., enrollment record) after successful transmission to IDMS. The confirmation of deletion will produce an auditable record of the event for verification.

Facilities and equipment will be secured by limiting physical access to the workspace and system, and by requiring an appropriate verification of identity for logical access to the system. Where appropriate, this method will use the TWIC credential providing one, two or three factors of authentication (i.e., something you have, something you know and something you are). Where absolutely necessary, this method will consist of two components (e.g., user_id + password). IDMS will also send confirmed TWIC application information to the card production facility via a private connection. Cards that are not active cannot be used for access to secure areas. Cards are deactivated when they are reported lost, stolen, damaged beyond use, or when a cardholder has failed to meet the terms and conditions of enrollment. Prototype demonstration

will be used to assess all aspects of the system in advance of full-scale implementation. TWIC is a developing program, which may have to be modified in the future. It is reasonable to expect some variations in the TWIC system, and as a result, this PIA may need to be updated to reflect these variations. Furthermore, information will be protected in accordance with the following requirements:

- The Privacy Act of 1974, as amended, (5 USC 552a), which requires federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of information protected by the Act.

- Federal Information Security Management Act of 2002, (Public Law 107-347), which establishes minimum acceptable security practices for federal computer systems. Additional details concerning security safeguards are described in greater detail later in this document.

- International Committee for Information Technology Standards (INCITS) 383 Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers. This standard specifies the application profile in support of identification and verification of transportation workers, through the use of Biometric data collected during enrollment, at local access points (i.e., doors or other controlled entrances) and across local boundaries within the defined area of control.

Will the information be retained and if so, for what period of time?

After Prototype has ended, TSA will evaluate the results of the test and request appropriate retention schedules according to decisions made concerning full-scale implementation of the program.

To fulfill these objectives, TSA is currently developing a record retention schedule for approval by the National Archives and Records Administration (NARA) for records pertaining to this program relevant to both Prototype and full-scale implementation as appropriate. Once the records schedule is approved, TSA will amend this document to include the retention period for TWIC records.

Will the information collected be used for any purpose other than the one intended?

No. TSA ensures that this will be accomplished through legal agreements with its contractors and in compliance with the Privacy Act and the published system of records notices, and to support local statutory requirements, such as those found in Florida. Measures will be employed to protect equipment, facilities, material, and information systems. These measures will include: locks, ID badges, fire protection, redundant power and climate control to protect IT equipment.

How will the worker seek redress?

During Prototype, a redress process will not be instituted, because participation in this phase of the TWIC Program is voluntary and access privileges are not granted or denied by TSA.

Employees in Florida, who are required to undergo a criminal history records check pursuant to State law, are covered by any redress procedures established by the State of Florida. TSA is in the process of developing a robust redress process in preparation for the next phase of the program.

Which databases will the names be run against?

During the name-based security threat assessment, TSA will run the volunteer applicant's biographical information against terrorist-related databases to determine if an individual poses or is suspected of posing a threat to transportation security.

Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?

Yes. During Prototype, information will be processed at the Sensitive but Unclassified (SBU) level. See below for additional information on appropriate training.

- Personnel Background Checks – Government personnel requiring access to sensitive information must undergo the appropriate level of background investigation and obtain any security clearance necessary to gain access to data collected during Prototype.
- Training – All TSA and assigned contractor staff working on Prototype will complete mandatory privacy and security training commensurate with their responsibilities. TSA and its contractors will receive training on the requirements of the Privacy Act and TSA's Privacy Policy as it pertains to the handling of personal data specifically related to Prototype.
- Sensitive Information - All TSA employees and assigned contractors will be trained concerning the treatment of sensitive material. All sensitive material will be handled commensurate with federal guidelines for storing, accessing, sharing, copying, and transmitting sensitive information. Although these guidelines are for security purposes, they also add another layer of privacy protection to the candidate information.

What technical safeguards are in place to secure the data?

The technical controls describe the automated security features that protect information during processing, transmission, and storage.

- User Identification – TWIC cardholders will be authenticated to access the TWIC system using, at a minimum, two-factor authentication. A required component (first factor) of this authentication will be a TWIC. In combination with the TWIC, the second factor of this authentication may require a password, biometric (e.g., fingerprint), or a Personal Identification Number (PIN).
- User Groups – System users will be only be allowed to access information and features of the system appropriate for their level of job responsibility and level of security clearance.

These rights will be determined by the identification provided when authenticating (i.e., user identification) to the system as described above.

- Network Firewall – Equipment and software will be deployed to prevent intrusion into sensitive networks and computers.
- Encryption – Sensitive data will be protected by rendering it unreadable to anyone other than those with the correct keys to reverse the encrypted data.
- Audit Trails – Attempts to access sensitive data will be recorded for forensic purposes if an unauthorized individual attempts to access the information contained within the system.
- Recoverability – The system will be designed to continue to function in the event that a disaster or disruption of service should occur.
- Physical Security – Measures will be employed to protect equipment, facilities, material, and information systems. These measures will include: locks, ID badges, fire protection, redundant power and climate control to protect IT equipment.

A complete Information Assurance and Security plan will be developed and implemented for the TWIC Prototype demonstration. All technical measures and operational procedures will be consistent with federal law and DHS policy to provide information security strategy, technology and process documentation, directives on roles and responsibilities, management policies, operational policies, and application rules. These measures will be applied to communications between component systems, interfaces between component systems and external systems. A periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability will also be required. Any system users acting as an operator of the system will be officially designated as agents of the government and will be required to complete a training process to ensure that they are trained and qualified to conduct business between the government and citizens, where public trust is required. Varying levels of responsibility and access to system functions will be delineated through user roles; systems users other than TWIC applicants and enrollees are referred to as TWIC Trusted Agents throughout program planning documentation and referenced as TSA Contractors throughout this PIA. These individuals will be authorized representatives of the government and will be subject to the details described earlier in this section.

- **Contact Point and Reviewing Official**

Contact Point: Lisa S. Dean, Privacy Officer, Transportation Security Administration
Reviewing Official: Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Department of Homeland Security

ATTACHMENT A

U.S. Department of Justice
Immigration and Naturalization Service

OMB No. 1115-0136

Employment Eligibility Verification

INSTRUCTIONS

PLEASE READ ALL INSTRUCTIONS CAREFULLY BEFORE COMPLETING THIS FORM.

Anti-Discrimination Notice. It is illegal to discriminate against any individual (other than an alien not authorized to work in the U.S.) in hiring, discharging, or recruiting or referring for a fee because of that individual's national origin or citizenship status. It is illegal to discriminate against work eligible individuals. Employers **CANNOT** specify which document(s) they will accept from an employee. The refusal to hire an individual because of a future expiration date may also constitute illegal discrimination.

Section 1 - Employee. All employees, citizens and noncitizens, hired after November 6, 1986, must complete Section 1 of this form at the time of hire, which is the actual beginning of employment. **The employer is responsible for ensuring that Section 1 is timely and properly completed.**

Preparer/Translator Certification. The Preparer/Translator Certification must be completed if Section 1 is prepared by a person other than the employee. A preparer/translator may be used only when the employee is unable to complete Section 1 on his/her own. However, the employee must still sign Section 1.

Section 2 - Employer. For the purpose of completing this form, the term "employer" includes those recruiters and referrers for a fee who are agricultural associations, agricultural employers or farm labor contractors.

Employers must complete Section 2 by examining evidence of identity and employment eligibility within three (3) business days of the date employment begins. If employees are authorized to work, but are unable to present the required document(s) within three business days, they must present a receipt for the application of the document(s) within three business days and the actual document(s) within ninety (90) days. However, if employers hire individuals for a duration of less than three business days, Section 2 must be completed at the time employment begins. **Employers must record: 1)** document title; **2)** issuing authority; **3)** document number, **4)** expiration date, if any; and **5)** the date employment begins. Employers must sign and date the certification. Employees must present original documents. Employers may, but are not required to, photocopy the document(s) presented. These photocopies may only be used for the verification process and must be retained with the I-9. **However, employers are still responsible for completing the I-9.**

Section 3 - Updating and Reverification. Employers must complete Section 3 when updating and/or reverifying the I-9. Employers must reverify employment eligibility of their employees on or before the expiration date recorded in Section 1. Employers **CANNOT** specify which document(s) they will accept from an employee.

- If an employee's name has changed at the time this form is being updated/ reverified, complete Block A.
- If an employee is rehired within three (3) years of the date this form was originally completed and the employee is still eligible to be employed on the same basis as previously indicated on this form (updating), complete Block B and the signature block.
- If an employee is rehired within three (3) years of the date this form was originally completed and the employee's work authorization has expired **or** if a current employee's work authorization is about to expire (reverification), complete Block B and:
  - examine any document that reflects that the employee is authorized to work in the U.S. (see List A **or** C),
  - record the document title, document number and expiration date (if any) in Block C, and
  - complete the signature block.

Photocopying and Retaining Form I-9. A blank I-9 may be reproduced, provided both sides are copied. The Instructions must be available to all employees completing this form. Employers must retain completed I-9s for three (3) years after the date of hire or one (1) year after the date employment ends, whichever is later.

For more detailed information, you may refer to the INS Handbook for Employers, (Form M-274). You may obtain the handbook at your local INS office.

Privacy Act Notice. The authority for collecting this information is the Immigration Reform and Control Act of 1986, Pub. L. 99-603 (8 USC 1324a).

This information is for employers to verify the eligibility of individuals for employment to preclude the unlawful hiring, or recruiting or referring for a fee, of aliens who are not authorized to work in the United States.

This information will be used by employers as a record of their basis for determining eligibility of an employee to work in the United States. The form will be kept by the employer and made available for inspection by officials of the U.S. Immigration and Naturalization Service, the Department of Labor and the Office of Special Counsel for Immigration Related Unfair Employment Practices.

Submission of the information required in this form is voluntary. However, an individual may not begin employment unless this form is completed, since employers are subject to civil or criminal penalties if they do not comply with the Immigration Reform and Control Act of 1986.

Reporting Burden. We try to create forms and instructions that are accurate, can be easily understood and which impose the least possible burden on you to provide us with information. Often this is difficult because some immigration laws are very complex. Accordingly, the reporting burden for this collection of information is computed as follows: **1)** learning about this form, 5 minutes; **2)** completing the form, 5 minutes; and **3)** assembling and filing (recordkeeping) the form, 5 minutes, for an average of 15 minutes per response. If you have comments regarding the accuracy of this burden estimate, or suggestions for making this form simpler, you can write to the Immigration and Naturalization Service, HQPDI, 425 I Street, N.W., Room 4034, Washington, DC 20536. OMB No. 1115-0136.

EMPLOYERS MUST RETAIN COMPLETED FORM I-9
PLEASE DO NOT MAIL COMPLETED FORM I-9 TO INS

U.S. Department of Justice
Immigration and Naturalization Service

OMB No. 1115-0136

Employment Eligibility Verification

Please read instructions carefully before completing this form. The instructions must be available during completion of this form. ANTI-DISCRIMINATION NOTICE: It is illegal to discriminate against work eligible individuals. Employers CANNOT specify which document(s) they will accept from an employee. The refusal to hire an individual because of a future expiration date may also constitute illegal discrimination.

Section 1. Employee Information and Verification. To be completed and signed by employee at the time employment begins.

Print Name: Last	First	Middle Initial	Maiden Name

Address *(Street Name and Number)*	Apt. #	Date of Birth *(month/day/year)*

City	State	Zip Code	Social Security #

I am aware that federal law provides for imprisonment and/or fines for false statements or use of false documents in connection with the completion of this form.

I attest, under penalty of perjury, that I am (check one of the following):

- ☐ A citizen or national of the United States
- ☐ A Lawful Permanent Resident (Alien # A_____)
- ☐ An alien authorized to work until ___/___/___
  (Alien # or Admission #) _____

Employee's Signature	Date *(month/day/year)*

Preparer and/or Translator Certification. *(To be completed and signed if Section 1 is prepared by a person other than the employee.) I attest, under penalty of perjury, that I have assisted in the completion of this form and that to the best of my knowledge the information is true and correct.*

Preparer's/Translator's Signature	Print Name

Address *(Street Name and Number, City, State, Zip Code)*	Date *(month/day/year)*

Section 2. Employer Review and Verification. To be completed and signed by employer. Examine one document from List A OR examine one document from List B and one from List C, as listed on the reverse of this form, and record the title, number and expiration date, if any, of the document(s)

List A	OR	List B	AND	List C
Document title: _____		_____		_____
Issuing authority: _____		_____		_____
Document #: _____		_____		_____
Expiration Date *(if any)*: ___/___/___		___/___/___		___/___/___
Document #: _____				
Expiration Date *(if any)*: ___/___/___				

CERTIFICATION - I attest, under penalty of perjury, that I have examined the document(s) presented by the above-named employee, that the above-listed document(s) appear to be genuine and to relate to the employee named, that the employee began employment on *(month/day/year)* **___/___/___ and that to the best of my knowledge the employee is eligible to work in the United States. (State employment agencies may omit the date the employee began employment.)**

Signature of Employer or Authorized Representative	Print Name	Title

Business or Organization Name	Address *(Street Name and Number, City, State, Zip Code)*	Date *(month/day/year)*

Section 3. Updating and Reverification. To be completed and signed by employer.

A. New Name *(if applicable)*	B. Date of rehire *(month/day/year) (if applicable)*

C. If employee's previous grant of work authorization has expired, provide the information below for the document that establishes current employment eligibility.

Document Title: _____ Document #: _____ Expiration Date (if any): ___/___/___

I attest, under penalty of perjury, that to the best of my knowledge, this employee is eligible to work in the United States, and if the employee presented document(s), the document(s) I have examined appear to be genuine and to relate to the individual.

Signature of Employer or Authorized Representative	Date *(month/day/year)*

LISTS OF ACCEPTABLE DOCUMENTS

LIST A

Documents that Establish Both Identity and Employment Eligibility

1. U.S. Passport (unexpired or expired)
2. Certificate of U.S. Citizenship *(INS Form N-560 or N-561)*
3. Certificate of Naturalization *(INS Form N-550 or N-570)*
4. Unexpired foreign passport, with *I-551 stamp or* attached *INS Form I-94* indicating unexpired employment authorization
5. Permanent Resident Card or Alien Registration Receipt Card with photograph *(INS Form I-151 or I-551)*
6. Unexpired Temporary Resident Card *(INS Form I-688)*
7. Unexpired Employment Authorization Card *(INS Form I-688A)*
8. Unexpired Reentry Permit *(INS Form I-327)*
9. Unexpired Refugee Travel Document *(INS Form I-571)*
10. Unexpired Employment Authorization Document issued by the INS which contains a photograph *(INS Form I-688B)*

OR

LIST B

Documents that Establish Identity

1. Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address
2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address
3. School ID card with a photograph
4. Voter's registration card
5. U.S. Military card or draft record
6. Military dependent's ID card
7. U.S. Coast Guard Merchant Mariner Card
8. Native American tribal document
9. Driver's license issued by a Canadian government authority

For persons under age 18 who are unable to present a document listed above:

10. School record or report card
11. Clinic, doctor or hospital record
12. Day-care or nursery school record

AND

LIST C

Documents that Establish Employment Eligibility

1. U.S. social security card issued by the Social Security Administration *(other than a card stating it is not valid for employment)*
2. Certification of Birth Abroad issued by the Department of State *(Form FS-545 or Form DS-1350)*
3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
4. Native American tribal document
5. U.S. Citizen ID Card *(INS Form I-197)*
6. ID Card for use of Resident Citizen in the United States *(INS Form I-179)*
7. Unexpired employment authorization document issued by the INS *(other than those listed under List A)*

Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)