Privacy Impact Assessment
for the

Transportation Worker Identification Credential Program

May 9, 2006

<u>Contact Point</u>
John Schwartz
TWIC Program Manager
Transportation Security Administration
571-227-2177

<u>Reviewing Officials</u>
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
(571) 227-3654

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The Transportation Security Administration is publishing a joint Notice of Proposed Rulemaking (NPRM) with the U.S. Coast Guard to implement a Transportation Worker Identification Credential (TWIC) program to provide a biometric credential that can be used to confirm the identity of workers in the national transportation system. TSA will conduct a security threat assessment before issuing the credential. TSA expects to collect identifying information, supporting documentation, a digital photograph, and fingerprints, as more fully set forth below in section 1.1. This PIA reflects the TWIC Program as proposed in the NPRM and follows on the PIA for the TWIC Prototype, which was published at www.dhs.gov on November 5, 2004. The program – and this PIA – are expected to change in response to public comment on the NPRM. A revised PIA and Final Rule will be issued prior to any collection of information.

Introduction

As proposed in the NPRM, the purpose of the TWIC program is to ensure that only authorized personnel who have successfully completed a security threat assessment have unescorted access to secure areas of maritime facilities and vessels. The credential will include a reference biometric -- fingerprints -- that positively links the credential holder to the identity of the individual who was issued the credential. At any time, TWIC holders may be asked to confirm, by providing a fingerprint, that they are the rightful owner of the credential. Access control procedures and systems at facilities and vessels will recognize the credential and the information encrypted on it, so that the overall maritime network will be interoperable. TSA has designed the TWIC process to maintain strict privacy controls to prevent a TWIC holder's biographic and biometric information from being compromised.

Individuals must enroll for a TWIC at a designated enrollment center. However, to reduce the time needed to complete the entire enrollment process at an enrollment center, an individual may pre-enroll via the Internet by providing limited biographical data. The applicant can access the TWIC website to provide personal information required for enrollment and select an enrollment center at which to complete enrollment. Applicants who pre-enroll must appear at enrollment centers to verify their identity, confirm that the information provided during pre-enrollment is correct, provide biometrics, and sign the enrollment documents. TSA, or TSA's agent operating under TSA's direction, will conduct the TWIC enrollment. All enrollment personnel must successfully complete a TSA security threat assessment and receive a TWIC before they will be authorized to access documents, systems, or secure areas. Following enrollment, the TSA system sends pertinent parts of the record to various sources so that appropriate terrorist threat, criminal history, and immigration checks can be performed. When the checks are completed, TSA makes a determination whether or not to issue a TWIC to the applicant and notifies the applicant.

When TSA has determined that an applicant is qualified to receive a TWIC, the TSA system generates an order to produce a credential. The TWIC is produced at a government credential production facility and shipped by express carrier to an enrollment center specified by the applicant. Once delivered to the enrollment center, the applicant will be advised to come to enrollment center to be issued the credential. Once issued, the TWIC is ready to be used as an access control tool. Possession of a TWIC does not guarantee access to secure areas because the owner/operator controls which individuals are given unescorted access to the facility or vessel. Rather, TWIC is a secure, verified credential that can be used in conjunction with the owner/operator's risk-based security plan and as required by the Coast Guard security regulations. Because the Coast Guard has jurisdiction over ports and maritime facilities, the TWIC program is a coordinated effort between the Coast Guard and TSA.

Because this program entails a new collection of information about members of the public in an identifiable form, the E-Government Act of 2002 and the Homeland Security Act of 2002 require that TSA conduct a Privacy Impact Assessment (PIA). The data collected and maintained for this program and the details on uses of this information are outlined in this Privacy Impact Assessment.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

An applicant for a TWIC will be required to provide his/her full name and previous names used; address; contact phone number; date of birth; place of birth; employer name and address; job title; gender; height, weight, eye and hair color; immigration status; and alien registration number, if applicable; visa number, country of citizenship. The applicant will be asked to provide his/her Social Security number. Providing the Social Security number is voluntary, but failure to do so may delay or prevent completion of the security threat assessment. For applicants who choose to pre-enroll, they will be able to provide biographical data described above in order to expedite the enrollment process. At the enrollment center, each applicant must provide identity documents, as detailed in Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) Form I-9 (Employment Eligibility Verification), to prove the claimed identity. TSA will also collect the applicant's digital photograph and fingerprints (ten prints).

1.2 From whom is information collected?

The information will be collected, either online through pre-enrollment or at an enrollment center, from transportation workers who require unescorted access to secure areas of vessels and maritime facilities.

1.3 Why is the information being collected?

The biographic and biometric information collected will be used to conduct a security threat assessment that includes a criminal history records check, immigration status checks, and a check of the terrorist database, as required by the Maritime Transportation Security Act (MTSA) (Pub.L. 107-295, Nov. 25, 2002). The fingerprints will be used to verify identity of the holder of the credential and the photograph will be collected so that it can be printed on the TWIC card as a means to identify the cardholder The TWIC, once issued, will be used continually by the cardholder to access secure areas of maritime facilities and vessels.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The program implements authorities set forth in the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71; Nov. 19, 2002; sec. 106), the Maritime Transportation Security Act of 2002 (MTSA) (Pub. L. 107-295; Nov. 25, 2002; sec. 102), and the Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users (SAFETEA-LU) (Pub. L. 109-59; Aug. 10, 2005; sec. 7105), codified at 49 U.S.C. 5103a(g). TSA is issuing a joint NPRM with the U.S. Coast Guard applicable to the maritime transportation sector that would require this information collection. TSA and Coast Guard will issue a final rule after consideration of any public comments received in response to the NPRM.

1.5 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

TSA is collecting the personal data to conduct security threat assessments, to verify identity, to determine eligibility for a TWIC, and to issue a TWIC. The applicant's name and photograph will be printed on the card, and biometric data (fingerprint templates) and the PIN will be stored on the card's integrated circuit chips. Data on the credential is encrypted. It cannot be read unless there is mutual authentication between the credential and the reader. No data will be transmitted beyond the local facility when the credential is read. Biometric data is PIN-protected on the contact chip.

For applicants who choose to pre-enroll, the data submitted via the Internet will be sent using Internet security protocols. All information provided is then stored in the TSA system, which encrypts the data at very high standards before it is transferred or stored, and protects the data from unauthorized access. If an enrollment center temporarily loses its Internet connection, the enrollment data is encrypted and stored on the enrollment workstation, but only until an Internet connection is restored. Limiting the personal data received by TSA to that necessary to conduct the types of checks required and for the foregoing purposes serves the agency's operational purposes while minimizing the privacy risks for individuals who have access to secure areas of U.S. port facilities and vessels.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Following enrollment, the TSA system sends pertinent parts of the record to various sources so that appropriate terrorist threat, criminal history, and immigration checks can be performed. The information will be used to initiate the security threat assessment to ascertain that an applicant's claimed identity is his real identity, to determine that the applicant does not pose a security threat, to determine eligibility for a TWIC, and to issue a TWIC.

When the checks are completed, TSA makes a determination whether or not to issue a TWIC to the applicant and notifies the applicant. Where TSA has determined an applicant is qualified to receive a TWIC and notifies the applicant, the TSA system generates an order to produce a credential. The TWIC is produced at a government credential production facility and shipped to an enrollment center for activation and issuance. Once received by the applicant, the TWIC is ready to be used as an access control tool. For circumstances where TSA has determined an applicant is not qualified to receive a TWIC because TSA has determined the applicant poses a security threat, see section 7.2.

The TWIC security threat assessment and credential are valid for five years, unless derogatory information is discovered and TSA revokes the credential. TSA will routinely update the security threat assessment on all credential holders; the fingerprint-based criminal history records check is conducted once every five years. A list of invalid credential numbers is available to facility operators in order to restrict access to those individuals that no longer qualify for a TWIC.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The information will be provided in person by the applicant to a TWIC Trusted Agent (TA), who will input the data in an electronic format. The applicant will review the data entered by the TA for accuracy before it is transmitted. The identity verification documents are scanned into the TSA system. Individuals who choose to electronically pre-enroll must bring the necessary identity verification documents to the enrollment center to complete enrollment.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The risk of compromise of personal information was considered throughout the TWIC system design. For applicants who choose to pre-enroll, the data submitted via the Internet will be sent using Internet security protocols. All information provided is then stored in the TSA system, which encrypts the data at very high standards before it is transferred or stored, and protects the data from unauthorized access. If an enrollment center temporarily loses its Internet connection, the enrollment data is encrypted and stored on the enrollment workstation, but only until an Internet connection is restored. TWIC enrollment stations were designed to provide privacy during the data collection by preventing unauthorized individuals from viewing screens containing personal information.

All collected data will be electronically stored in one location, and no paper copies will be maintained. The data collected during enrollment will be encrypted before transmission and then transmitted to the TSA system over a secure internet connection. The data is then automatically deleted from the Trusted Agent enrollment workstation. Once the information is sent to TSA, the information will be forwarded to the various interfaces to conduct the security threat assessment. After the card production facility produces the credential, the data will be automatically deleted from the card production facility system. Personal information collected will not be stored outside the TSA system except when it is actually being used by other parts of the system.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives in accordance with record schedules to be submitted for approval by the National Archives and Records Administration (NARA).

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Section 1.1 describes the data collected by TSA. There are three points in the process at which data is collected; the enrollment center, the TSA system, and the card production facility. As explained in section 2.4, data collected at the enrollment center will be deleted at the enrollment center when it is transmitted to TSA. Data will be deleted from the card production facility after the credential is produced. This leaves only the TSA system as the site for retention of information. While a retention schedule has not yet been determined at this NPRM stage, it is expected to be retained there for at least five years to coincide with the expiration of the TWIC. A final retention schedule will be determined in conjunction with the final rulemaking.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

TSA will share information with U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), and with the U.S. Coast Guard. The information TSA receives from TWIC applicants also may be shared with DHS employees and DHS contractors that have a need to know the information in order to carry out their official duties, including but not limited to immigration, law enforcement or intelligence operations. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

4.2 For each organization, what information is shared and for what purpose?

TSA will share information within DHS for purposes of card production, immigration checks, and port access. Biographic and biometric information also will be shared with those employees that have a need to know the information in order to carry out their official duties, including but not limited to immigration, law enforcement or intelligence purposes. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

4.3 How is the information transmitted or disclosed?

TSA will transmit biographic and biometric data via a secure data network, secure facsimile, or password protected CD. Other information, including status of a credential, may be transmitted by telephone. The method of transmission may vary according to specific circumstances. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Information is shared within DHS with those individuals who have a need for the information to perform their official duties in accordance with the Privacy Act. Privacy protections include strict access controls, including security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

TSA will share information with the Terrorist Screening Center (TSC) as part of the threat assessment. TSA will also share information with Federal agencies for purposes of performing criminal checks. TSA may share information with Federal, state, or local law enforcement or intelligence agencies or other organizations in accordance with the Privacy Act and the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (TSTAS). This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735.

Pursuant to MTSA, TSA may notify an applicant's employer if TSA determines that the applicant poses a security threat and disqualifies an applicant. However, pursuant to MTSA, TSA will not provide any of the applicant's biographical data (other than the applicant's name) collected during enrollment or the reason for the disqualification to the individual's employer. TSA will only make available a list of invalid credential numbers to facility operators to enable them to determine if a credential has been revoked or reported lost or stolen.

5.2 What information is shared and for what purpose?

Biographic and biometric data collected from TWIC applicants will be sent to Federal agencies for criminal history records checks, immigration and terrorism checks, and may be sent to other Federal databases as necessary to complete the security threat assessment. Data will also be sent to a Federal card production facility to generate the credential. When an individual is identified as a threat, it is expected that that individually identifying data and security threat assessment status about that individual will be shared, as needed, with Federal, State, or local enforcement or intelligence agencies to communicate the threat assessment results and to facilitate an operational response. Further, pursuant to MTSA, the individual's name and results of an individual's security threat assessments, but not the other biographical data or reason for the adverse determination, may be shared with the individual's employer.

5.3 How is the information transmitted or disclosed?

TSA will transmit biographic or biometric data via a secure data network, secure facsimile, or password protected CD. Other information, including status of a credential may be transmitted by telephone. The method of transmission may vary according to specific circumstances. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes. TSA currently has an MOU with USCIS for immigration checks and will establish an MOU with the FBI and the Terrorist Screening Center (TSC) prior to the exchange of any information. TSA also intends to enter into an MOU with USCIS in connection with card production prior to the exchange of any information, so that a USCIS facility can produce the cards.

5.5 How is the shared information secured by the recipient?

TSA shares information in accordance with the Privacy Act. Federal agencies and their contractors are subject to the safeguarding requirements of the Privacy Act and under the Federal Information Security Management Act, Title III of the E-Government Act, Pub. L. 107-347 (FISMA).

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

None. However, TSA requires the data to be handled in accordance with the Privacy Act and/or any other applicable handling restrictions and TSA personnel handling the data are required to complete the required TSA Privacy training prior to handling personally identifiable information.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

TSA will share this information under the applicable provisions of the Privacy Act. By limiting the sharing of this information to those who have an official need to know it and by sharing only in accordance with published routine uses or under the Privacy Act, TSA is mitigating any attendant privacy risks. Further, TSA has entered into, or will have in place, MOUs governing the conditions of sharing information as discussed in section 5.4. TSA will not provide any of the applicant's biographical data collected during enrollment or the reason for the disqualification to the individual's employer. Further, data will be deleted at the enrollment center when transmitted to TSA. Data will be deleted from the card production facility after the card is produced.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. At the enrollment center, applicants will receive a Privacy Act Statement and consent form, by which they agree to provide personal information for the security threat assessment and credential. For applicants who pre-enroll, the Privacy Act Statement is provided with the application on-line, but the applicants must acknowledge receipt of the notice in writing at the enrollment center. If an applicant fails to sign the consent form or does not have the required documents to authenticate identity, enrollment will not proceed. As TWIC is implemented, TSA and Coast Guard will make information available to affected workers in advance of enrollment so that all are aware of what to bring to the enrollment center. This information will also be posted on the TSA/TWIC website, which is www.twicprogram.com. All information collected at the enrollment center or during the pre-enrollment process, including the signed Privacy Act Statement and consent form and identity documents, is scanned into the TSA system for storage. All information is encrypted or stored using methods that protect the information from unauthorized retrieval or use. Further, this PIA and the NPRM serve to provide notice.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

With the exception of a Social Security number (SSN), if individuals choose not to provide the information, they will be ineligible to receive a TWIC, and therefore will be denied unescorted access to secure areas of transportation facilities and vessels. Individuals may choose to refuse to provide a SSN, but such refusal may result in delays in processing their application and completing the security threat assessment.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No. However, if TSA determines the individual poses a security threat, all uses of such information by TSA will be consistent with the Privacy Act and the DHS/TSA 002, Transportation Security Threat Assessment System SORN identified in paragraph 5.1 above.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

TSA is collecting only the information provided by the applicant that is minimally required to verify the applicant's identity, determine eligibility for a TWIC, conduct the required security threat assessment, and issue a TWIC. Individuals are provided with meaningful notice that enables them to exercise informed consent prior to disclosing any information to TSA.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration
TSA-20,WestTower
FOIA Division
601South12thStreet
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting erroneous information?

If it is determined that a TWIC applicant may pose a security threat, TSA will notify the applicant by mailing an Initial Determination of Threat Assessment (IDTA) containing the reason(s) for the issuance of the IDTA and directions as to how the applicant may submit an appeal. The appeal must be submitted within sixty days after the date of service of the IDTA or sixty days from TSA's response to the applicant's request for further information pertaining to the determination.

An applicant may appeal an IDTA by: 1) serving TSA with a written answer that includes relevant agency or court documents to verify the applicant's identity and correct errors in the applicant's records; or 2) requesting a copy of the documents on which TSA based its Initial Determination. No documents that are classified or otherwise protected by law will be released. TSA will release as much information to the applicant as permitted by law to provide for a meaningful appeal.

The appeal process consists of a review of the IDTA, the materials upon which the decision was based, the applicant's appeal materials and any other relevant information or material available to TSA. An appeal of an IDTA based on disqualifying criteria will be reviewed and decided by the TSA Director or designee. When an Initial Determination is made that an applicant does not qualify for a TWIC, and the applicant appeals the decision, the Assistant Secretary or designee will review the case and make the Final Determination.

Upon review of the appeal, the Assistant Secretary or Director may overturn the Initial Determination and serve a Withdrawal of the Initial Determination on the applicant, or uphold the Initial Determination and issue a Final Determination of Threat Assessment to the applicant.

Individuals believed to pose an imminent security threat will receive Initial Determination of Threat Assessment and Immediate Revocation (hereinafter "Immediate Revocation"). The Immediate Revocation will be sent to the employer at the same time and to the U.S. Coast Guard to deny the individual access to the facility. Individuals wishing to appeal an Immediate Revocation will follow the appeal processes outlined above. Information regarding the appeals procedures will be provided to individuals whom TSA determines to pose an imminent security threat. If an individual fails to initiate an appeal within sixty days after receipt, the Immediate

Revocation becomes final, and TSA serves a Final Determination of Threat Assessment upon the U.S. Coast Guard and the individual's employer.

7.3 How are individuals notified of the procedures for correcting their information?

The Initial Determination of Threat Assessment letter sent to the applicant will contain the procedures for submitting appeals.

7.4 If no redress is provided, are alternatives are available?

If an appeal results in a Final Determination of Threat Assessment because of a disqualifying criminal offense or a past declaration of mental incompetence, the applicant may request a waiver. The applicant must submit a request for a waiver within sixty days after service of the Final Determination of Threat Assessment. Applicants who are associated with terrorists or terrorist activity or who are in the country illegally are not eligible for a waiver. In addition, applicants convicted of certain particularly serious felonies, such as treason, espionage, or sedition, or conspiracy to commit the foregoing, are not eligible for a waiver. Waivers are offered because an applicant may be rehabilitated to the point that he or she can be trusted in sensitive or potentially dangerous work or has been declared mentally competent. The NPRM provides criteria that TSA considers if the individual does not meet the criminal history standards. TSA believes that these factors are good indicators that an individual may be rehabilitated to the point that a waiver is advisable. The factors are: (1) the circumstances of the disqualifying act or offense; (2) restitution made by the individual; (3) Federal or State mitigation remedies; (4) court records indicating that the individual has been declared mentally competent; and (5) other factors TSA believes bear on the potential security threat posed by an individual. Many of these factors are set forth in MTSA, at 46 U.S.C. 70105(c)(2).

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

TSA has incorporated processes for allowing individuals to access and correct their records, and to allow for appeals and waivers.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

In order to perform their duties in managing, upgrading, and using the system, system administrators, security administrators, IT specialists, vetting operators and analysts have access to the system. Role-based access controls are employed to limit the access of information by different users and administrators based on the need to know. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. This system is used internally within DHS and provides no public access. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. TSA also follows DHS Sensitive Systems Policy Publication 4300A and TSA IT Security Policies 1400.2 for handling of data.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors who are hired by DHS to perform many of the IT maintenance and security monitoring tasks have access to the system in order to perform their official duties. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. All contractors are subjected to requirements for suitability and a background investigation under TSA Management Directive 1400.3, TSA Information Security Policy. New contracts will be awarded when the system is implemented. Contractors operating a system of records to accomplish a TSA function will be required to adhere to the Privacy Act. Current IT system contracts contain Privacy Act clauses.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, role-based access controls are employed to limit the access of information by different users and administrators based on the need to know.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The system will be secured against unauthorized use through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards. This is documented in the System Security Plan currently under development as mandated by the Federal Information Security Management Act of 2002, Pub.L.107-347 (FISMA) following National

Institute of Standards and Technology (NIST) guidance. The System Security Plan will be completed prior to implementation of the program. The systems are also assessed and audited on an annual and ad hoc basis by the IT Security Office.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Employees or contractors are assigned roles for accessing the system based on their function. TSA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained through TSA's Security and Awareness Training Program when they join the organization and periodically thereafter. The status of personnel who have completed the training is reported to TSA on a monthly basis. The Facility Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Trusted Agents and card production facilities do not retain applicant data once the information is transferred to the TSA system. Transmission, receipt, and subsequent deletion of data is automatic and auditable. The system also employs real-time auditing functions to track real-time users. Data is encrypted at rest and in transmission.

The system is secured against unauthorized use through the use of a layered defense, in-depth security approach involving procedural and information security safeguards. This is documented in the System Security Plan currently under development. The System Security Plan will be completed prior to implementation of the program.

All TSA and DHS employees and assigned contractor staff receive DHS-mandatory privacy training on the use and disclosure of personal data. They also receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

All government and contractor personnel must be approved for access to the facility where the system is housed, issued picture badges with embedded integrated proximity devices and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides overall guidance on how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of the Rules of Behavior prior to getting access to any IT system.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All government and contractor personnel are required to complete the on-line TSA Privacy Training, which includes a discussion of Fair Information Practices (FIPs) and instructions on handling personally identifiable information in accordance with FIPs and TSA Privacy Policies. Compliance with this training requirement is audited monthly by the TSA Privacy Officer, and failure to complete the training is reported to program management. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information. All IT security training is reported as required in the Federal Information Security Management Act of 2002, Pub.L.107-347 (FISMA).

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Information in this system will be safeguarded in accordance with the FISMA. All systems will operate on legal authority of the Designated Accrediting Authority (DAA) and will complete necessary security artifacts for this approval and required for Certification and Accreditation.

This system will be certified and accredited prior to achieving operational status. This system will be reviewed for major changes and certification documentation will be updated to reflect all technical security controls in alignment with the FIPS 199 categorization.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

TSA has implemented security controls and technological features that fully incorporate privacy. TSA will comply with FISMA prior to operating.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

This system was designed using standards-based system architecture. Commercially available programs were joined with custom software code to create the TWIC information technology system. All TWIC system hardware was commercially purchased and installed.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The data stored in the various technologies used in the credential, such as magnetic stripe, and contactless chip technologies is protected in accordance with Federal Information Processing Standard (FIPS) 201-1. FIPS 201-1 provides detailed requirements for Personal Identity Verification programs required to comply with Homeland Security Presidential Directive (HSPD)-12. The fingerprint data, which is the reference biometric, is used to match the credential to the person who enrolled. The TWIC card system enables the use of biometrics to verify access rights rather than storing extensive amounts of personal information on the card.

The TWIC system contains many feedback mechanisms to validate the transmission and receipt of data at key points in the process. Whenever data is transmitted to or from the TWIC central information processing system the transmission is recorded within the system to provide an audit trail.

Credentials are electronically locked during the production process so that the data cannot be altered once the credential leaves the production facility. The TWIC security threat assessment and credential are valid for five years, unless derogatory information is discovered and TSA revokes the credential. TSA will routinely update the security threat assessment on all credential holders; the fingerprint-based criminal history records check will be conducted once every five years.

All biographic and biometric data are securely stored in one TSA location. Further, biometric data is segmented and stored separately from the biographic data to ensure privacy.

9.3 What design choices were made to enhance privacy?

In addition to the discussion in 9.2 above, the only personal identifying information contained on the credential is a name and a photo of the individual. The fingerprint template stored on the credential cannot be used to develop a fingerprint image—another privacy protection. In compliance with FIPS 201, the fingerprint template stored on the contact chip is not released to readers until the card PIN is first input.

9.4 Privacy Impact Analysis

System data is segmented and segregated to limit access to biometric data. Access to a single segment will not provide access to other segments. The TWIC program has served as a model for the development of Federal Information Processing Standards Publication 201 (FIPS 201), which requires any personal identity verification system, of which TWIC is one, to be implemented in strict accordance with the privacy laws and policies of the Federal government.

Conclusion

Since its inception, the TWIC program's three goals have been to improve security, enhance commerce, and protect personal privacy. TSA has carefully chosen the methods of collecting personal information from applicants, of transmitting it through various TWIC modules, and of storing it to balance individual privacy rights with the Government's need to verify personal identity and assess one's suitability for access to secure areas of the Nation's transportation system. The TWIC program has served as a model for the development of Federal Information Processing Standards Publication 201 (FIPS 201), which requires any Personal Identity Verification system for Federal employees or contractors to be implemented in strict accordance with the privacy laws and policies of the Federal government. TWIC has been developed to protect the privacy of those who seek unescorted access to secure areas of transportation facilities and vessels.

Responsible Official

John Schwartz

Transportation Security Administration

Arlington, Virginia 22202

571-227-2177

Approval Signature Page

____

Peter Pietra

Director, Privacy Policy and Compliance

Transportation Security Administration

____________________________________ May 9, 2006

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security