Privacy Impact Assessment
for the

Transportation Worker Identification Credential Program

October 5, 2007

Contact Point
John Schwartz
TWIC Assistant Director
Transportation Security Administration
571-227-4545

Reviewing Officials
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) published a joint Final Rule with the United States Coast Guard (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, and conducted a Privacy Impact Assessment (PIA) associated with that Final Rule. TSA is amending the PIA to reflect the development of TWIC contactless card capability in sections 1.4, 1.6, 9.2 and 9.3, and the approval of the records schedule by NARA in section 3. This PIA replaces the one published December 29, 2006.

Introduction

As set out in the Final Rule, 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. Commercial drivers licensed in Mexico and Canada transporting hazardous materials in accordance with 49 CFR 1572.201 may also apply for a TWIC. The credential will include a reference fingerprint biometric that positively links the credential holder to the identity of the individual who was issued the credential. As designed and proposed in the NPRM, TWIC can be used in conjunction with access control readers designed to recognize the credential and the information encrypted on it to permit authorized individuals to enter secure areas of port facilities and vessels without escort. However, many commenters raised questions about the durability of the readers in a commercial and/or marine environment and the potential delays that might result from the proposed entrance procedures. As a result, the Final Rule does not require the installation of card readers at this time. Initially, TWIC will be visually inspected by owner/operators at access points rather than read by an automated reader. In addition, the Coast Guard will conduct random and periodic checks at access control points. The rule also permits personnel of the Department of Homeland Security (DHS), National Transportation Safety Board, and law enforcement officers to conduct audits to confirm that the credential is held by an authorized individual. It is expected that TWIC will be used with access control systems in the future. TSA has designed the credential and 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 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. All applicants, including those who pre-

enroll, must appear at an enrollment center 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 TWIC enrollment. All enrollment personnel will successfully complete a TSA security threat assessment before being authorized to access documents, systems, or secure areas.

Following enrollment, the TSA system sends pertinent parts of the record to the FBI, as well as within DHS, so that appropriate terrorist threat, criminal history, and immigration checks can be performed. TSA reviews the results of the checks to determine whether the individual poses a security threat, and notifies the applicant of the result. When TSA has determined that an applicant is qualified to receive a TWIC, the TSA system generates an order to produce a credential. The credential is produced at a federally managed production facility and shipped to the center where the applicant enrolled. The TSA system notifies the applicant that his or her TWIC is ready for pick-up and the applicant must return to the enrollment center to retrieve and activate the credential. At this time, applicants will select a personal identification number (PIN), which is programmed into the card and serves as an added layer of security for the biometric data embedded on the credential.

Commenters expressed the need to provide vessel and facility owners/operators with the ability to put new, direct hires to work immediately if an urgent staffing requirement exists, after new hires have applied for their TWIC. As a result of the comments, the Final Rule permits new, direct hires to have limited access to secure areas for up to 30 consecutive days, provided the conditions described in the rule are met. For these individuals, the operator's Facility or Vessel Security Officer will be required to re-enter their limited biographic information directly into the U.S. Coast Guard's Homeport web portal. The Homeport web portal is a Coast Guard system designed for secure communications by the Coast Guard, maritime industry, Area Maritime Security Committees, and other entities regulated under the Maritime Transportation Security Act (MTSA) of 2002. TSA will be notified by Homeport of these individuals. New, direct hires will not be permitted to access ports or facilities until the facility receives interim clearance status from TSA.

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 program that is required in security regulations issued by the Coast Guard. TSA will make available only a list of invalid credential numbers to facility and vessel operators for use in insuring that holders of revoked credentials are not able to access secure areas without an escort.

This program entails a new collection of information about members of the public in an identifiable form, thus the E-Government Act of 2002 and the Homeland Security Act of 2002

require TSA to 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. This PIA replaces the one published December 29, 2006.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

TWIC applicants must provide full name and previous names used; address; email address, if available; contact phone number; date of birth; place of birth; employer name and address if working for the employer requires obtaining a TWIC (and, if the applicant's current employer is the U.S. military service, branch of the service); job title and description; gender; height, weight, eye and hair color; immigration status; if applicable, alien registration number and/or the number assigned on U.S. Customs and Border Patrol Arrival-Departure Record form I-94; if applicable, visa number, type, expiration date, and country of citizenship. An applicant who is a credentialed mariner or applying to become a credentialed mariner must include proof of citizenship in the identity verification documents, as well as their merchant mariner documentation or license), which TSA will scan into the enrollment record and transmit to the Coast Guard. The Coast Guard requires proof of citizenship in order to obtain a merchant mariner license. Applicants who are commercial drivers licensed in Canada or Mexico who are applying for a TWIC in order to transport hazardous materials in accordance with 49 CFR 1572.201 and not to access secure areas of a facility or vessel, must explain this when applying and present their hazardous materials endorsement (HME) license.

For new, direct hires who have not yet received a TWIC and to whom vessel and facility owners/operators wish to grant limited access to secure areas of the facility in the meantime, the Facility or Vessel Security Officer must enter the following information into the Coast Guard's Homeport web portal: 1) full name; 2) date of birth; 3) Social Security Number (optional); 4) employer name and 24-hour contact information; and 5) date of TWIC enrollment.

Applicants will be asked to provide additional information that can shorten the time it takes to complete adjudication. Applicants may provide their Social Security number (SSN); failure to provide it may delay or prevent completion of the security threat assessment. Also, applicants may provide their passport number, city of issuance, date of issuance and the expiration date. If born abroad, applicants may provide the Department of State Record of Foreign Birth. Applicants will be asked whether they 1) have previously completed a TSA threat assessment, and if so the date and program for which it was completed; and 2) currently holds a federal security clearance, and if so, the date of and agency for which the clearance was

performed. This information is particularly important in the case of an applicant who seeks to have TSA issue a comparability determination.

Applicants who pre-enroll online can provide the biographic data described above in order to expedite the enrollment process, but all applicants must come to an enrollment center to verify identity, sign the application, provide fingerprints (ten prints), and have a digital photograph taken.

TSA also collects certain information as a result of the checks performed against terrorist threat, criminal history, and immigration databases. If the individual has a criminal record, a copy of that record will be collected. For other databases, the result of the check will be collected. As discussed below in section 7, other information may be collected in connection with the redress, appeal, or waiver process.

1.2 From whom is information collected?

The information will be collected from all credentialed merchant mariners and individuals who wish to obtain unescorted access to secure areas of a regulated facility or vessel. Also, information will collected from applicants who are commercial drivers licensed in Canada or Mexico who are applying for a TWIC in order to transport hazardous materials in accordance with 49 CFR 1572.201. Finally, if an owner/operator wishes to place a new employee in the secured area immediately, the Facility or Vessel Security Officer must input the employee's biographic information described in Section 1.1 into the Coast Guard Homeport web portal.

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 identity verification checks, criminal history records checks, immigration status checks, and terrorist database checks on individuals who have unescorted access to secure areas of ports and thereby require a TWIC as required by the Maritime Transportation Security Act (MTSA) (Pub.L. 107-295, Nov. 25, 2002). The additional information provided voluntarily may expedite the adjudication process for applicants who are born abroad or for applicants who have already completed a federal security threat assessment. The fingerprints will be used to verify the 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. Fingerprints will also be stored in the U.S. VISIT IDENT system for use in accordance with the system of records notices and PIAs applicable to TWIC and IDENT. The IDENT PIA may be found at www.DHS.gov. The information collected via the Coast Guard Homeport web portal will be used to assist the Coast Guard and TSA in identifying new, direct

hires who are awaiting TWIC issuance. The TWIC, once issued, will be used by the cardholder to access secure areas of maritime facilities and vessels.

1.4 How is the information collected?

Personal information is collected through the on-line pre-enrollment process, if used, and/or the enrollment process at enrollment sites operated by personnel under contract to TSA. TSA does not routinely gather information regarding TWIC usage, though if there were an incident implicating transportation security, and if the facility used a card reader and maintained records on card use, then TSA might seek card usage records for investigative or forensic purposes. Facility and vessel operators may choose to use card readers to assist in managing access to their facilities or vessels.

1.5 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 and the Coast Guard published an NPRM for the TWIC program on May 22, 2006. After consideration of public comments received in response to the NPRM, TSA and the Coast Guard are issuing a joint Final Rule that requires this information collection.

1.6 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 (or to determine if a background check conducted by another governmental agency is comparable to the standards in the Final Rule in order to minimize redundant background checks of workers), to verify identity, to determine eligibility for a TWIC, and to issue a TWIC.

Data on the credential is encrypted and cannot be read or compromised unless there is mutual authentication between the credential and the reader. When the credential is presented for access, no data is transmitted to TSA or the Coast Guard.

Personal information can be obtained from a TWIC in three ways: 1) viewing information printed on the card; 2) reading information from the card's chip using a contact reader; and, 3) reading information from the card's chip using a contactless reader. The

applicant's name and photograph can be viewed whenever the TWIC is presented or displayed. For contact readers, the individual's name, digital photo, biometric data (fingerprint templates) and personal identification number (PIN) is stored on the card's chip. This information is protected through the use of the individual's PIN which must be entered before the information is released to a contact reader. For contactless readers, only the individual's biometric data can be read. The biometric data is protected from unintended disclosure by both storing and transmitting it in an encrypted format. A decryption key is needed to read or use the biometric data. The decryption key, called the TWIC Privacy Key (TPK), is stored on the card's magnetic strip and contact chip interface. The TPK can only be provided to the contactless reader by swiping the magnetic stripe or inserting the card into a contact reader (no PIN required) to retrieve the TPK. The applicant's biometric data is thus prevented from being gathered by eavesdropping during the contactless transmission to a reader. In addition, the biometric is a fingerprint template rather than a fingerprint image, and cannot be reversed to create a original fingerprint.

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 or hashes all personally identifying information 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. The Coast Guard Homeport web portal, which owner/operators will use to submit personal information concerning new, direct hires is designed for secure communications. Limiting the amount of personal data TSA receives to what is necessary to conduct a security threat assessment and satisfy MTSA serves the agency's operational purposes and minimizes the privacy risks for TWIC applicants.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Enrollment personnel review identity verification documents to prevent the use of fraudulent identity documents. The TSA system sends pertinent parts of the enrollment record to the FBI, as well as within DHS, so that appropriate terrorist threat, criminal history, and immigration checks can be performed. TSA reviews the results of the checks to determine whether the individual poses a security threat and is eligible to hold a TWIC, and then notifies the applicant of the result. When applicable, TSA reviews pertinent information to determine whether a comparable threat assessment was completed. Upon a TSA determination that a comparable threat assessment was completed, the applicant may pay a reduced fee.

When TSA has determined that an applicant is qualified to receive a TWIC and notifies the applicant, the TSA system generates an order to produce a credential. A TWIC is produced at a credential production facility and shipped to the center at which the applicant enrolled. Once the enrollment center receives the credential, the applicant will be notified to return to the enrollment center to retrieve and activate the credential.

In cases where TSA has determined an applicant is not qualified to receive a TWIC, the applicant has the opportunity to appeal the decision, and in some cases may request a waiver. See section 7.2 for a full discussion of the redress process. If the applicant does not pursue an appeal or waiver, or if the adverse determination stands, TSA notifies the Federal Maritime Security Coordinator (FMSC), who may be the Captain of the Port, that the individual was denied a TWIC. In addition, TSA notifies the Coast Guard in the case of applicants who are mariners and are denied a TWIC. Finally, TSA may notify an applicant's employer of the denial if TSA determines that the applicant poses an imminent threat. Generally, TSA will not disclose the reason for the denial.

If an owner/operator wishes to have a new, direct hire work in the secure area before the security threat assessment is complete and a TWIC is issued, the owner/operator must submit the employee's information (described in 1.1) to the Coast Guard's Homeport. TSA will conduct an interim check and will notify the owner/operator if the employee poses a security threat and cannot be granted unescorted access to secure areas.

The TWIC credential is valid for five years, unless derogatory information is discovered during the five years and TSA revokes the credential. TSA will routinely update the security threat assessment on all credential holders. 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 the enrollment personnel, who will input the data in an electronic format. The applicant will review the data entered for accuracy before it is transmitted. The identity verification documents are scanned

into the TSA system. To the extent the information entered into the Coast Guard web portal requires verification, TSA expects the facility or vessel owner/operator to check the information for accuracy before it is submitted.

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 design of the TWIC system. 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 or hashes all personally identifying information 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 secure locations, 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 identity verification and security threat assessments. After the card production facility produces the credential, the data will be automatically deleted from the card production facility 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 approved by the National Archives and Records Administration (NARA). TSA will retain records for individuals who are not a match or potential match to a watchlist for one year after the individual no longer has access. In addition, for those individuals who may originally have appeared to be a match to a watch list, but subsequently cleared, TSA will retain the records for at least seven years, or one year after access has been terminated. For individuals who are an actual match to a watch list or otherwise determined to pose a threat to transportation security, TSA will retain the records for 99 years, or seven years after TSA learns that an individual is deceased.

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

Yes, on March 8, 2007.

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

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 also be deleted from the card production facility after the credential is produced. TSA has developed a record retention schedule for Transportation Threat Assessment and Credentialing records, of which these records are a part. The retention periods are designed to retain the information while the individual is an active TWIC holder, or to permit review of records for individuals who may have been cleared as a match to a watch list only after more extensive review. It is also designed to permit TSA to detect fraudulent multiple applications.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

TSA will routinely share information within TSA's Office of Transportation Threat Assessment and Credentialing (TTAC), U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), and the Coast Guard. The information TSA receives from TWIC applicants also may be shared with DHS employees and DHS contractors that have a need for the information in the performance of 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 biographic, biometric, and status information within TTAC and USCIS for purposes of identity verification, criminal history checks, card production, port access, and audit purposes. TSA will share biographic and biometric information with CBP, USCIS and ICE for immigration checks. TSA will share biographic, biometric, and status information with the

Coast Guard for purposes of port access and auditing. Biographic, biometric, and status information also will be shared with those employees that have a need for the information in the performance of their official duties, including but not limited to identity verification, 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, applicant or credential status and other information in person, via a secure or encrypted data network, via facsimile, on a password-protected CD or by telephone. The method of transmission may vary according to specific circumstances, and will be in accordance with OMB guidance regarding the transmission and storage of personal information.

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 in the performance of 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 TSA 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 FBI to conduct criminal history record checks. TSA may also share information with the Terrorist Screening Center (TSC) and with other 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. TSA may also share information with the applicant's employer and port or facility owner/operators.

5.2 What information is shared and for what purpose?

TSA may share biographic information with the Terrorist Screening Center (TSC) during the security threat assessment process. Biographic and biometric data collected from TWIC applicants will be sent to other Federal agencies for identity verification, criminal history records checks, immigration and terrorism checks, and may be sent to other Federal databases as necessary to complete the security threat assessment. When an individual is identified as a threat, it is expected 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, TSA and the Coast Guard are not authorized to provide the reason for the adverse determination to the individual's employer.

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 and other information as necessary to identify the individual) collected during enrollment or the reason for the disqualification to the individual's employer. TSA will provide owner/operators a list of invalid credential numbers, not names or other identifying information, to enable them to determine if a credential has been revoked or reported lost or stolen.

TSA will share the information 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).

5.3 How is the information transmitted or disclosed?

TSA will transmit biographic or biometric data, applicant or credential status and other information in person, via a secure or encrypted data network, via facsimile, password-protected CD, or by telephone. The method of transmission may vary according to specific circumstances and will be in accordance with OMB guidance on the handling of personal information.

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 an MOU with the FBI and the Terrorist Screening Center (TSC), which reflects the scope of the information shared. TSA also has entered 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. TSA and the Terrorist Screening Center (TSC) entered into an MOU on May 12, 2006. Information may be shared in accordance with the applicable SORN listed above, DHS/TSA 002 Transportation Security Threat Assessments, or in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.

5.5 How is the shared information secured by the recipient?

Any Federal agency and their contractors receiving this information are expected to handle it in accordance with the Privacy Act and that agency's applicable SORNs. In addition, Federal agencies and their contractors are subject to information security requirements of 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 is required. However, any Federal agency receiving this information is expected to handle it in accordance with the Privacy Act, that agency's applicable SORNs, and FISMA.

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 DHS personnel and contractors who have a need to know it in the performance of their official duties 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 MOUs governing the conditions of sharing information as discussed in section 5.4. TSA will not provide employers with the applicant's biographic data collected during enrollment (other than name and other information as necessary to identify the individual) or the reason for the disqualification. 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. 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 personally identifying information is encrypted or hashed to protect the information from unauthorized retrieval or use. Further, this PIA and the Final Rule serve to provide notice. The applicable Privacy Act system of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (TSTAS) was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735.

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

Yes, applicants provide information voluntarily, but individuals who do not provide the information will be ineligible to receive a TWIC, and therefore would not have unescorted access authority to secure areas of facilities and vessels. SSN is a voluntary item of information. For individuals who choose to refuse to provide a SSN, 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. 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 will be requiring the collection of information 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. In response to public comment on the NPRM, TSA will permit individuals to submit additional information that will assist in adjudicating their application. TSA has weighed the privacy risks associated with collecting additional information against the potential for delays in adjudicating the TWIC application. Given the significance of any delay in granting the TWIC, and the security infrastructure associated with the enrollment process, TSA has concluded that individuals should be permitted to submit additional information, such as passport number and country and city of issuance. Individuals will be 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
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by email at FOIA.TSA@dhs.gov. 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/research/foia/index). 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 TSA determines 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 determination and directions on how the applicant may appeal it. The applicant may initiate an appeal by submitting a written reply to TSA, a written request for materials from TSA, or by requesting an extension of time. If the applicant does not initiate an appeal within 60 days of receipt of the IDTA, it generally becomes final. Applicants may request an extension of the deadline after it has passed by filing a motion describing the reasons why they were unable to comply with the timeline. Individuals who may be out at sea or are otherwise unable to collect mail in a timely fashion may request an extension of the deadline after the deadline has passed by filing a motion describing the reasons why they were unable to comply with the timeline.

If the applicant requests documents, TSA will release as much information to the applicant as permitted by law to provide for a meaningful appeal. No documents that are classified or otherwise protected by law will be released.

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 criminal or immigration information will be decided by the TSA Assistant Administrator or designee. When an Initial Determination is made that an applicant does not qualify for a TWIC under section 1572.107 of the rule, and the applicant appeals the decision, the Assistant Secretary or designee will review the case and make the Final Determination.

The Assistant Secretary or Assistant Administrator may overturn the IDTA and serve a Withdrawal of the Initial Determination on the applicant, or uphold the IDTA and issue a Final Determination of Threat Assessment to the applicant and when applicable, to the licensing State, the Coast Guard, or the appropriate FMSC. Individuals who unsuccessfully appeal a disqualification based on intelligence information may then appeal to an Administrative Law Judge (ALJ).

Individuals believed to pose an imminent security threat will receive Initial Determination of Threat Assessment and Immediate Revocation (hereinafter "Immediate Revocation"). If appropriate, TSA will notify law enforcement, the Coast Guard, and the

employer to minimize the risk that the applicant can access the secure area without escort. Individuals wishing to appeal an Immediate Revocation will follow the appeal processes outlined above.

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

The IDTA includes the procedures for submitting an appeal.

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

Applicants who are disqualified because of a disqualifying criminal offense or a past declaration of mental incompetence, or are not eligible to apply for a TWIC because they are aliens in Temporary Protected Status (TPS), may request a waiver. If disqualified by TSA, the applicant must submit a waiver request within sixty days after service of the Final Determination of Threat Assessment. Individuals who may be out at sea or are otherwise unable to collect mail in a timely fashion may request an extension of the deadline after the deadline has passed by filing a motion describing the reasons why they were unable to comply with the timeline. In addition, applicants may re-apply for a waiver if TSA denies a waiver request any time. 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.

The following factors are important in TSA's consideration of a waiver request: (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).

Individuals who are denied a waiver may request review of the waiver denial by an ALJ within 30 calendar days from the date of service of TSA's decision. Applicants may request an extension of the deadline after the deadline has passed by filing a motion describing the reasons why they were unable to comply with the timeline. The ALJ who conducts the review will possess the appropriate security clearance necessary to review classified or otherwise protected information and evidence. The procedures for review are set out in the Final Rule. The ALJ's decision may be appealed by either party to the TSA Final Decision Maker (who is the TSA Assistant Secretary, acting in the capacity of the decision maker on appeal, or any person to whom the Assistant Secretary has delegated his or her decision-making authority) within 30 calendar days of service of the decision of the ALJ. A person may seek judicial review of a final

order of the TSA Final Decision Maker as provided in 49 U.S.C. 46110. A party seeking judicial review of a final order must file a petition for review not later than 60 days after the final order has been served on the party.

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, adjudicators, enrollment personnel 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. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is enforced by the system in coordination with and through oversight by TSA security officers.

For details concerning the technical access and security of the Homeport web portal, please see the PIA for this Coast Guard system, which was published on May 9, 2006.

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.

Yes, DHS will hire contractors to perform many of the IT maintenance and security monitoring tasks have access to the system in order to perform their official duties. Contractors are under obligations to follow the privacy and security requirements of the Department.

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. These procedures are documented in Standard Operating Procedures (SOP) and also referenced in the System Security Plan, 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 systems are also assessed and audited on an annual and ad hoc basis by the TSA IT Security Office.

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

Security Administrators for the TWIC system assigns roles and rules. 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.

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

Enrollment personnel and enrollment center equipment do not retain applicant data once the information is transferred to the TSA system. The card production facility does not retain applicant data once the card is produced and mailed. Transmission, receipt, and subsequent deletion of data is performed on a recurring basis and governed by Quality Assurance Procedures. The system also employs real-time auditing functions to track real-time users.

The system is secured against unauthorized use through the use of a layered defense, in-depth security approach involving procedural and information security safeguards. The TWIC program is currently developing the System Security Plan, which documents this. 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 personnel are required to complete the on-line TSA Privacy Training Course. Contract personnel who are responsible for maintaining the TWIC system within TSA's government facility will be badged by TSA and also complete the on-line TSA Privacy Training Course. Compliance with this training requirement is audited monthly by the TSA Privacy Officer, and failure to complete the training is reported to program management. TWIC Trusted Agents, who are also contract personnel, will receive TSA Privacy Training as part of the Trusted Agent Training Course.

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 by 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 FISMA. The TWIC system will operate on legal authority of the Designated Accrediting Authority (DAA) who manages personnel, operations, maintenance, and budgets for the system or field site. The DAA will complete necessary security artifacts for this approval and required for Certification

and Accreditation. The Coast Guard's Homeport system has been accredited by the Coast Guard DAA.

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. The FIPS 199 categorization was completed November 17, 2006.

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 technology features that fully incorporate protection of privacy. TSA has complied with FISMA, and mitigated privacy risks through the following methods:

-- Access to the system is controlled through role based user accounts.

-- The system access through user accounts is auditable.

-- The system strictly controls the transmission and storage of data.

-- All government and contract personnel are required to complete privacy training (see 8.7 above).

-- The system is audited by TSA Security Personnel to ensure FISMA compliance.

Section 9.0 Technology

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

Commercially available programs were integrated 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.

For the contact interface of the card, the data stored in the various technologies used in the credential, such as 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. For the contactless interface of the card, the data is protected from access through the use of the TWIC Privacy Key (TPK) developed in cooperation between TWIC and the maritime and technology sectors. The TPK solution is based on the E-Passport Basic Access Control protocol. The fingerprint data, which is the reference biometric, is used to match the credential to the person who enrolled. TSA has determined to use biometrics to verify access rights for the TWIC card system 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 is 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.

All biographic and biometric data collected is electronically stored in secure locations. 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?

-- The enrollment stations are designed to prevent non-authorized individuals from seeing an applicant's personal information

--There is no paper record created or kept by TSA or its contractor that contains an applicant's personal information.

--The personally identifying information is stored electronically in segments and is encrypted or hashed so that it would not be useful even if an individual with ill intent gained access to it.

--The list of revoked cards does not include any personal information, only the credential number.

--Completed credentials are 'locked' until activated at the enrollment center by a Trusted Agent and the applicant.

--Biometric data available via the contactless interface is protected by an industry recommended TWIC Privacy Key based on the E-Passport Basic Access Control protocol.

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. No other personal information is stored on the credential.

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 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 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.

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security