Privacy Impact Assessment
for U.S. Port Access Threat Assessments

April 28, 2006

Contact Point

Stephen Sadler
Director, Maritime and Surface Credentialing
Transportation Security Administration
(571) 227-3603

Reviewing Officials

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

Introduction

Under 50 U.S.C. 191 and 33 C.F.R. part 125, the United States Coast Guard is requiring individuals to present identification credentials for access to waterfront facilities and port and harbor areas, including vessels and harbor craft in those areas. Pursuant to 33 C.F.R. §125.15(a), the Commandant of the Coast Guard directed the Captains of the Port (COTP)[1] to prevent access to all facilities regulated under 33 C.F.R. part 105 by persons who do not have an approved identification credential listed in 33 C.F.R. §125.09 or other approved credential. Approved identification credentials for port facility operator employees and longshoremen are a facility employee identification card, a state-issued driver's license, or a personal identification issued by the individual's employer, union, or trade association, provided that the individual is screened by the Transportation Security Administration (TSA) and does not pose or is not suspected of posing a security threat warranting denial of access to the port facility. "Facility operator employees" include all permanent employees and long-term contractors who need regular access to the facility for a period in excess of ninety days.

To accomplish screening of the facility operator employees and longshoremen, facility operators and longshore unions were directed by the U.S. Coast Guard (USCG) to provide to TSA full name, date of birth, social security number, and alien registration number, where applicable, to conduct a security threat assessment on each individual. In conjunction with the USCG's statutory mandate, TSA has broad authority under 49 U.S.C. §114(f) to assess threats and threat information and to plan and execute such actions as may be appropriate to address threats to transportation. The information may be submitted through the Coast Guard Homeport web portal or via direct transmission to TSA on a password-protected Compact Disk. 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. The system is used for transmission of security plans and as a communications tool in the event of natural disaster or other emergency. The Homeport system may also be used to transmit information needed for access to maritime facilities.

Because this program entails a new collection of information about members of the public in an identifiable form, the E-Government Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

TSA will collect the full name, date of birth, social security number, and alien registration number, where applicable, of all facility operator employees, long-term contractors, and longshoremen. Individuals will be compared to watch list information held by the Terrorist Screening Center in the Terrorist Screening Database (TSDB) and will be checked for immigration status. A redress process is available to individuals who are identified as a security threat. This process will entail the collection of additional information about the individual necessary to resolve any issues regarding misidentification. The additional

[1] The COTP is authorized to direct Coast Guard Law Enforcement activity with the port.

information sought will vary based on the reasons for any misidentification. The redress process is more fully explained in section 7.2 below

1.2 From whom is information collected?

U.S. port facility operators and longshore unions are required to enter the biographic information directly into the U.S. Coast Guard's Homeport web portal or send the information directly to TSA on a password-protected compact disk (CD). TSA will access and retrieve data directly from the Homeport web portal.

1.3 Why is the information being collected?

The purpose of collecting this information is to perform a security threat assessment to ensure that individuals who are allowed access to U.S. port facilities do not pose or are not suspected of posing a threat to transportation security.

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

Under 50 U.S.C. 191 and 33 C.F.R. part 125, the U.S. Coast Guard is requiring individuals to present identification credentials for access to waterfront facilities and port and harbor areas. Pursuant to 33 C.F.R. §125.15(a), the Commandant of the Coast Guard directed the Captains of the Port to prevent access to all facilities regulated under 33 C.F.R. part 105 by persons who do not have an approved identification credential listed in 33 C.F.R. §125.09 or other approved credential. A requirement to have an approved credential includes a security threat assessment conducted by TSA. Under 49 U.S.C. §114(f), TSA has broad authority to carry out transportation security responsibilities, including assessing threats to transportation security.

1.5 Privacy Impact Analysis

TSA is limiting the personal data it receives to those elements necessary to conduct the security threat assessments. Limiting the personal data received by TSA serves the agency's operational purposes while minimizing the privacy risks for individuals who have or are seeking access to secure areas of U.S. port facilities.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

TSA will use the information to conduct security threat assessments for the purpose of identifying actual or potential threats to transportation security.

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

No.

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

Port facility operators and longshore unions will provide the information to TSA from their existing files to the extent possible. In that case, it will be presumed that facility operator, contractor employee files and longshore union files contain accurate names, dates of birth, social security numbers, and alien registration numbers, where applicable. To the extent the information requires verification, TSA expects the facility operator or longshore union to check the information for accuracy before it is submitted. If the facility operators or unions do not have all of the information requested in their existing files, they will collect the information directly from the individual. In such cases, TSA expects that the individual will provide accurate information.

2.4 Privacy Impact Analysis

The risk of collecting inaccurate information is minimized because employees, union members, facility operators or contractors, and longshore unions presumably have made efforts to correctly identify their employee or member names, dates of birth, and social security numbers, as well as alien registration numbers, where applicable. If the facility operators, contractors, or unions collect the information directly from the individual, the risk of collecting inaccurate information is also minimal because it is presumed that the individual will provide accurate information. Further, the impact of collecting inaccurate information is minimized because individuals who feel they have been wrongly identified as a security threat can seek redress through TSA allowing for an additional review of the completeness and accuracy of the information.

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

Information collected through this program will be maintained in accordance with NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The information TSA receives may be shared with DHS components 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?

As noted above, TSA may share name, date of birth, social security number, alien registration number if applicable, and results of comparisons to the TSDB and immigration checks within DHS where there is a need to know the information for immigration, law enforcement, intelligence, or other official purposes related to transportation security. 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 this data within DHS via a secure data network, secure facsimile, password-protected CD, or telephonically only to those who need the information to perform their official duties. This 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

Information is shared within DHS with those individuals who have demonstrated 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 TSC as part of the threat assessment and with Federal agencies for immigration checks. TSA will share the results of the threat assessment with the COTP and the longshore unions or facility operator. TSA may share the information it receives with Federal, state, or local law enforcement or intelligence agencies or other organizations, including port facility operators and longshore unions, in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA 002, Transportation Security Treat Assessment System (T-STAS). This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735.

5.2 What information is shared and for what purpose?

When an individual is identified as a security threat, it is expected that individually identifying data and security threat assessment status about the individual will be shared, as needed, with Federal, State, or local law enforcement or intelligence agencies and with port facility operators or longshore unions to communicate threat assessment results and to facilitate an operational response.

5.3 How is the information transmitted or disclosed?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed telephonically, electronically via a secure data network, via a secure facsimile, or via a password-protected CD.

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. Sharing of information between the TSA and TSC is subject to an MOU. That MOU reflects the scope of the information shared and imposes restrictions on use of the information. The Privacy Act System of Records Notice described above reflects the scope of the information that will be shared.

5.5 How is the shared information secured by the recipient?

TSA shares information in accordance with the Privacy Act of 1974. Federal agencies are subject to the safeguarding requirements of the Privacy Act and under the Federal Information Security Management Act (FISMA), Title III of the E-Government Act, Pub.L. 107-347.

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

TSA will share this information under the applicable provisions of the SORN and the Privacy Act. By limiting the sharing of this information to those who have an official need to know it and by ensuring that recipients properly handle this data, TSA is mitigating any attendant privacy risks.

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?

The Coast Guard is publishing a System of Records Notice for the Homeport web portal in conjunction with its Federal Register notice and serves as notice of the collection.

A majority of the information is being collected from the port facility operators and longshore unions who will obtain it to the extent possible from existing port facility or contractor employee personnel files or union files. Therefore, TSA did not provide notice to the individual prior to its collection by the port facility operator or union. In cases where the port facility operators, contractors or longshore unions do not have all of the information in their existing files, the information may be collected directly from the individual. Port facility operators or unions must provide a Privacy Act notice to those individuals prior to collecting the information. A copy of this notice may be found at Appendix A of this PIA. In addition, the publication of this PIA and of the SORN for DHS/TSA 002, Transportation Security Threat Assessment System, serve to provide public notice of the collection, use, and maintenance of this information. This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735. In the event that an individual is determined to be a security threat and the individual believes that the results of the screening are inaccurate, he or she will be informed by TSA on how to pursue redress from TSA.

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

Yes. A majority of the information at issue has already been collected by the port facility operators and longshore unions. The U.S. Coast Guard requires the port facility operators and longshore unions to

notify employees of its intent to submit employee or union member information for purposes of a security threat assessment, and notify employees or union members that they may decline to provide their social security numbers, but that such action may result in delays or make it impossible to complete the threat assessment. If the information is not in the facility operator, contractor, or union's existing files, then the individuals must be provided a Privacy Act notice, and the individual will have the opportunity to decline to provide the information.

If additional information is needed during the redress process, that collection will be voluntary. However, individuals will not be granted access to the affected port facilities unless they provide information that enables TSA to resolve their redress request.

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

If TSA determines that an 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

The limited amount of information to be received by TSA serves the agency's operational purposes while minimizing the privacy risks for individuals whose information will be used to determine their access to the port. The U.S. Coast Guard requires port facility operators and longshore unions to notify employees or union members of its intent to submit employee or union member information for purposes of a security threat assessment, and notify employees or union members that they may decline to provide their social security numbers, but that such action may result in delays or make it impossible to complete the threat assessment. In cases where the information is collected directly from the individual, a Privacy Act notice must be provided to the individual. The notice will explain the authority for the collection, the purpose of the collection, the voluntary nature of providing the information, and that failure to provide the information may result in a delay or make it impossible to complete the threat assessment.

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, West Tower

FOIA Division

601 South 12th Street

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?

Individuals identified as posing a security threat will receive an Initial Determination of Threat Assessment. Individuals who believe that they have been wrongly identified as posing a security threat have the opportunity to appeal an Initial Determination of Threat Assessment. The appeal must be submitted within 30 days after the date of service of the Initial Determination of Threat Assessment or 30 days from TSA's response to the individual's request for materials pertaining to the determination. The date of service is the date of personal delivery, the date shown on a certificate of service, or 10 days from the date of mailing if there is no certificate of service or date of electronic transmission.

An applicant may appeal an Initial Determination of Threat Assessment by: 1) serving TSA with a written answer to the Initial Determination of Threat Assessment that includes relevant agency or court documents to verify the applicant's identity and correct errors in his or her records; or 2) requesting a copy of the documents on which TSA based the Initial Determination. However, no documents that are classified or otherwise protected by law can be released. Nevertheless, 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 Initial Determination of Threat Assessment, 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 Initial Determination of Threat Assessment based on immigration status is reviewed and decided by the Director, Transportation Threat Assessment & Credentialing. Upon review of the appeal, the Director or TSA Assistant Secretary may overturn the initial determination and provide a Withdrawal of the Initial Determination to the applicant and a Determination of No Security threat to the port facility operator and longshore union (if the union, not the facility employer, provided the individual's information for a security threat assessment). Conversely, if the Director or TSA Assistant Secretary upholds an Initial Determination of Threat Assessment, TSA will issue a Final Determination of Threat Assessment to the applicant, the port facility operator, and the longshore union. For purposes of judicial review, the Final Determination constitutes a final TSA order. The port facility operator is then required to initiate action to deny the individual access to the port.

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 port facility operator and longshore union at the same time and to the U.S. Coast Guard Captain of the Port (COTP) to deny the individual access to the facility. Individuals wishing to appeal an Immediate Revocation must follow the appeal procedures established for individuals denied a hazardous materials endorsement under TSA's regulations, which are set forth in 49 CFR 1572.141(i).

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 30 days after receipt, the Immediate Revocation becomes final, and TSA serves a Final Determination of Threat Assessment upon the port facility operator and the COTP.

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

Individuals will receive in writing an Initial Determination of Threat Assessment that contains the procedures to be followed for correcting their information.

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

N/A. A redress process, as described in section 7.2 above, is provided for individuals who believe that they have been wrongfully identified as a threat.

7.5 Privacy Impact Analysis

Individuals may request access to or correction of their personal information pursuant to a redress process noted above.

Section 8.0 Technical Access and Security

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

Individual information is expected to be manually processed. Accordingly, system interaction is expected to be limited, and will likely implicate only TSA e-mail and word processing systems. Data related to the threat assessments will only be accessed by TSA personnel with a need to know in order to perform their official duties. It will be maintained securely on TSA's IT infrastructure, to which no public access is provided. Moreover, 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 for handling of data. Answers to the remaining questions describe TSA's IT system.

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 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 IT Security Officers. All contractors performing this work are subjected to requirements for suitability and a

background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

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

Yes. Role-based access controls are used for controlling access to the system using the policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

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

Limited system access will be provided for purposes of conducting these security threat assessments. Generally, the system is secured against unauthorized use through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards.

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 are vetted and approved access to the facility where the system is housed, issued picture badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides an overall guidance of 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.

8.5 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?

The system is continuously monitored to audit compliance with policy. Weekly logs are reviewed to ensure no unauthorized access has taken place. All IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office.

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 annual 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 requirement is audited monthly by the TSA Privacy Officer. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed. 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 TSA's record systems is safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. All systems are operating on the authority of the Designated Accrediting Authority (DAA). The TSA Net completed FISMA Certification and Accreditation on November 15, 2005. The TSA E-Mail Exchange system is operating under an Interim Authority to Operate, with C&A expected to be complete by May 2006.

8.9 Privacy Impact Analysis

Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity badges and biometrics. The system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

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

The system is built from Commercial Off the Shelf (COTS) products and customized applications or Government Off the Shelf (GOTS) products. System components include COTS hardware and operating systems with GOTS applications.

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

Security and privacy requirements were analyzed based on FIPS-199 methodology. FIPS-199 methodology categorizes a system as High, Medium, or low, depending on how important the function is to the agency. The result of that analysis was that the system was rated as HIGH for data integrity and availability. All security controls are applied in accordance with this rating.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA has limited its data collection to specific elements necessary for security vetting. TSA has developed an information technology infrastructure that will protect against inadvertent use of personally identifying information not required by the government. Access to data collected for this program will be strictly controlled; only TSA employees and contractors with proper access controls will have permission to use and view this information. TSA will not transmit or otherwise share this information with entities outside of DHS that are not listed in the routine uses in the T-STAS Privacy Act System of Records Notice which was published in the Federal Register. Additionally, the record system will include a real time audit function to track access to electronic information, and any infractions of information security rules will be dealt with appropriately. Strict incident response plans are adhered to. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

9.4 Privacy Impact Analysis

These conscious design choices will limit access to the personal information, thereby mitigating any possible privacy risks associated with this program.

Conclusion

TSA is performing these threat assessments for the purpose of assessing the risks to transportation security associated with allowing individuals to have access to U.S. port facilities. Privacy impacts associated with this have been minimized by limiting the information provided to TSA and employing appropriate technical and operational safeguards and requirements. If TSA makes any changes to this program or the data elements needed for conducting the relevant security threat assessments or other checks on individuals, those changes will be reflected in an amended version of this PIA.

Responsible Official

Stephen Sadler

Transportation Security Administration

Arlington, VA 22202

571-227-3603

APPENDIX 1

Privacy Act Notice

Authority: 49 U.S.C. §114, 50 U.S.C. §191, and 33 C.F.R. part 125 and authorize the collection of this information.

Purpose: DHS will use this information to conduct a security threat assessment on port facility employees, port facility long-term contractors, and longshoremen.

Routine Uses: The information will be used by and disclosed to DHS personnel and contractors or other agents who need the information to assist in activities related to port security. Additionally, DHS may share the information with port operators, Longshore unions, and law enforcement or other government agencies as necessary to identify and respond to potential or actual threats to transportation security, or pursuant to its published Privacy Act system of records notice.

Disclosure: Furnishing this information is voluntary. However, failure to furnish the requested information may delay or prevent the completion of your security threat assessment.