Privacy Impact Assessment
for the

Homeport

May 9, 2006

Contact Point
LCDR Karrie Trebbe
Homeport Project Officer
U.S. Coast Guard
202-267-0385

CWO3 Anthony Johnson
Privacy Specialist
U. S. Coast Guard
(202)475-3526

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

Introduction

The Maritime Transportation Security Act (MTSA) of 2002 establishes a comprehensive national system of transportation security enhancements to protect America's maritime community against the threat of terrorism without adversely affecting the flow of commerce through United States ports. The Department of Homeland Security (DHS) United States Coast Guard (USCG) is the lead Federal agency for maritime homeland security and has significant enforcement responsibilities under the MTSA. Among its duties under the MTSA, the Coast Guard requires that maritime security plans be developed for ports, vessels and facilities, and that those individuals with access to maritime facilities have credentials demonstrating their eligibility for such access.

Homeport, a new system of records under the Privacy Act of 1974, will facilitate implementation of these requirements. Representatives of the maritime industry, members of Area Maritime Security Committees, other entities regulated by the MTSA, USCG, and other users associated with a vessel, facility, or specific committee will be able to register and use Homeport. This tool will serve as an enterprise portal that combines secure information dissemination, advanced collaboration, and provides a public-facing interface for internal Coast Guard processes. It is an operational mission replacement for the current legacy internet system (www.uscg.mil).

Homeport has three main functions: 1) a secure means for regulated entities to submit and store security plans for approval; 2) a secure means by which facility operators may view lists of union personnel authorized to access their facility; and 3) a secure means for representatives from the maritime domain[1] to submit personal information to the Transportation Security Administration (TSA) needed to conduct background screening and credentialing. This final functionality of Homeport is likely to be of limited duration until the full implementation of a more formal credentialing program is developed and implemented by TSA .

If additional functionality is added to Homeport, this PIA will be updated to reflect the changes.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The information to be collected depends on the functionality of Homeport. For representatives of the maritime domain, members of Area Maritime Security Committees, and other entities regulated by the MTSA needing to set up an account to use the Homeport portal, the following mandatory personal

[1] **Maritime Domain** is all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances.

information will be collected: Full Name, Address (including) City, State, Zip, Country, Work/Home/Emergency Telephone Number, Email Address, and Alien Registration number, when appropriate. A Sponsor Name and Telephone Number is also required for individuals seeking access who have been recommended by a facility owner who has herself been previously screened or received registration information from a specific Coast Guard employee.

A registration may be approved for persons who request access in support of a pre-designated person or "Sponsor." Contractors working on security plans, facility or vessel security officers and their employees with security duties represent individuals in this category. The following general information is required: The Captain of the Port Zone, Company or Organization, and Role in the Maritime Industry.

For Coast Guard members who have a need to access Homeport during normal business operations related to maritime domain requirements or security related duties, the above fields are pre-populated using data from Direct Access, the Coast Guard's enterprise human resource system. In addition to the previously mentioned fields, the following information for Coast Guard members will be transferred from Direct Access: Employee ID, and Grade Level.

For purposes of screening individuals with access to facilities, the following personal information will be stored in the Homeport Portal: Full Name, Date of Birth, Social Security Number (optional), and Alien Identification number (if applicable).

The lists of maritime personnel authorized to access their facility will be made available through Homeport. The information is organized by union and facility and is only accessible to those individuals with a need to view that particular union or facility information.

1.2 From whom is information collected?

For individuals seeking access to use the Homeport portal for submitting required documentation, the information will be submitted directly by the individual.

For individuals seeking access to a maritime facility, biographical information will be collected from individuals or their employers or unions.

The lists of maritime personnel authorized to access their facility will come from TSA.

1.3 Why is the information being collected?

Information on individuals with access to Homeport is collected in order to allow the Coast Guard to validate the suitability, identity, and eligibility of those who request permission and/or have access to the system.

By law and regulation (50 U.S.C. 191, the Magnuson Act of 1950, and 33 C.F.R. Part 125, Identification Credentials) the Coast Guard requires individuals to present identification credentials for access to waterfront facilities and port and harbor areas, including vessels and harbor craft in those areas.

Information on individuals seeking access to the facility will be collected and maintained in order to allow TSA to conduct background screening. The system will assist transportation facilities in managing their security risks and accounting for access of authorized personnel to transportation facilities and activities. In addition to information provided by TSA to facility operators and individuals, the Coast Guard will provide facility operators with lists of vetted personnel sorted by union local affiliation. The facility operators will be able to retrieve a list of each union that they utilize to assist in managing registration and/or security risks under their area of responsibility.

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

Under 14 U.S.C 88 and 50 U.S.C. 191, the Coast Guard maintains the right to perform any and all acts necessary to rescue and aid persons and save property and to restrict port access during national emergencies.

Pursuant 33 CFR Part 125, the Coast Guard is directed to require individuals to present identification credentials for access to waterfront facilities and port and harbor areas, including vessels and harbor craft in those areas.

1.5 Privacy Impact Analysis

To maintain the security of Homeport, USCG must collect information from individuals to validate them as users. In order to ensure that individuals with access to waterfront facilities have appropriate credentials, USCG must also collect information for screening by TSA and maintain the results of the threat assessment. While the collection of information presents a privacy risk, to mitigate that risk, USCG has minimized the amount and type of information it collects from individuals. USCG will stop collecting information on individuals seeking access to ports once TSA's Transportation Worker Identification Credential (TWIC) is in place.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Information on individuals with access to Homeport is used to allow the Coast Guard to validate the suitability, identity and eligibility of those who request permission and/or have access to the system for the purpose of managing requirements under the Maritime Transportation Security Act,.

Information on individuals with access to facilities is used to assist the Transportation Security Administration (TSA) in verifying the identity and background of maritime workers, and to assist transportation facilities in managing their security risks and accounting for access of authorized personnel to maritime facilities and activities. The Coast Guard will provide additional assistance by providing facility operators with lists of vetted personnel sorted by union affiliation or corporate entity to further assist in registration and/or security risks.

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?

Individuals seeking to use the Homeport system will input their data directly into the system. This information is then checked and validated by the designated approving official at the local Coast Guard Captain of the Port before an account is approved and created. Local Coast Guard Captain of the Port personnel will review submissions for accuracy.

Personal information submitted by individuals with access to Homeport regarding background screening by TSA is submitted by the employer or union. This system will serve as a pass-through for screening related information. TSA is responsible for vetting the data and conducting follow-up to determine suitability for credentials.

2.4 Privacy Impact Analysis

USCG and TSA have identified the identifiable information required in order to conduct a threat assessment. The information is used solely to meet USCG and TSA's statutory requirements to conduct threat assessments for all personnel with access to U.S. ports. Technical security and access measures are in place to ensure that users have approved access and using the information in an appropriate manner. Details of the security measures can be found in Sections 7 and 8 of this PIA.

Section 3.0 Retention

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

Registration information collected by Homeport will be deleted from the system once an account is terminated.

Data related to threat assessment for maritime personnel will be retained for two years by USCG.

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

No. However, a submission for approval has been made to NARA for approval.

3.3 Privacy Impact Analysis

Homeport user information is needed until the account is terminated to allow access to the system and accountability. Data related to threat assessment for maritime personnel will be retained for two years to allow adequate time for implementation of the Transportation Workers Identification Credential (TWIC) system. Upon implementation of TWIC, the data will be purged and only the lists of maritime personnel authorized to access their facility will be maintained on Homeport .

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The information will be shared with TSA for threat assessment of maritime personnel. This information may also be shared with other 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?

The Coast Guard may share Name, Date of Birth, Social Security Number, and Alien Registration Number, if applicable, with TSA for screening of facility personnel for access verifications. The Coast Guard may also share this information with other parts of DHS where there is a need to know the information for national security reasons. This information will be shared in accordance with 5 U.S.C 552a(b)(1) of the Privacy Act.

4.3 How is the information transmitted or disclosed?

Information is transmitted/disclosed by granting access to the Homeport Internet Portal via a secure data network, secure facsimile, password protected CD, or telephonically. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

4.4 Privacy Impact Analysis

The system has been designed so that only those individuals with a need to know the information are provided access based upon their role in the organization.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Once individuals are vetted for each port, the lists of union personnel authorized to access their facility will be made available to maritime facility operators who need the information to confirm facility access. The information will not be organized by individual name.

5.2 What information is shared and for what purpose?

The following information will be provided in this fashion: union affiliation, individual's first and last name, port or facility so that facility managers know who is authorized to enter the facility.

5.3 How is the information transmitted or disclosed?

For list containing the names of union members, information will be posted on the secure Homeport Portal where only registered Maritime Facility Security Officers with a clear need to know will be granted access.

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?

No.

5.5 How is the shared information secured by the recipient?

Lists containing names of authorized maritime personnel will be located in a password-protected area of the secure Homeport Web Portal for Maritime Facility Security Officers to access to assist in management of registration and security risk related matters.

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

Individuals provided access to Homeport must read and sign a Non-Disclosure Agreement and are provided a notice on the secure portal regarding the appropriate use of the information they are about to view.

5.7 Privacy Impact Analysis

The lists of union personnel authorized to access their facility will be made available only to registered Maritime Facility Security Officers via a password-protected area in the Homeport Web Portal and only for that facility for which the Security Officer has responsibility. For example, security officer for Port A will only be able to see vetted personnel for Port A and not Ports B, C, or D. This will mitigate the security concerns associated with providing electronic lists to maritime facilities through other non-secure methods. The posted lists will consist of only names of individuals who were previously submitted by the same facility.

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. A Privacy Act System of Records Notice was published in the Federal Register on April 28, 2006 (Appendix A). A Privacy Act Statement was developed and posted on the collection screen and in the system (Appendix B).

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

Yes. However, failure to provide information may result in not being provided a Homeport account, and not be granted access to a facility.

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?

Registered users may grant or decline consent to other registered users to view their user profile through the Preference Option available in Homeport.

6.4 Privacy Impact Analysis

The Privacy Statement is available to all users of the Homeport Portal. The system has been set up so that users may decide whether or not their profile is shared in the system. Access to the information is mitigated by only allowing users with authorized access to view certain information.

Section 7.0 Individual Access, Redress and Correction

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

Authorized users can see their profile based on their registration information. Authorized public users will primarily access their data through their system profile. Military and civilian individuals would primarily access their data via the source system, Direct Access. Access to other information is by request to the system administrator.

7.2 What are the procedures for correcting erroneous information?

Individuals seeking to correct erroneous information may submit a request to correct data to the Project Manager at the Department of Homeland Security, United States Coast Guard Headquarters, Commandant (G-PRI), 2100 2nd ST. SW. Washington, DC 20593-0001.

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

E-mail notification will be made to registrants upon acceptance or denial of accounts. Comments pertaining to why an account was declined will appear in the e-mail message. Therefore, allowing for dialogue pertaining to personal data.

Notification, Record Access, and Contesting Record Procedures are established and provided in Privacy Act Systems of Record Notice DHS/CG-060, which was published in the Federal Register on 28 April, 2006. Individuals may choose to submit a Privacy Act Request to correct information on themselves. This guidance will be posted in the Privacy Statement on the Homeport Web-site.

TSA maintains the responsibility for addressing information correction for individuals registered through the screening program. Individuals will receive an Initial Determination of Threat Assessment, in writing, that contains the procedures to be followed for correcting their information.

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

Redress is provided as described in 7.3 above for individuals who believe information on themselves is incorrect.

7.5 Privacy Impact Analysis

The majority of the information provided through Homeport is related to facilities and/or assets rather than individuals. Most personal information will be related to user registration on Homeport or vetted maritime personnel. Individuals whose personal information is collected and used by the Homeport system may, to the extent permitted by law, examine their information and request correction of inaccuracies. The Coast Guard will invoke every administration and/or technical measure to ensure personal information is not misused, mishandled, and/or compromised.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Authorized Users, Managers, System Administrators, and Developers all have access. Access levels are driven by roles within the organization, need to know, eligibility, and suitability. These criteria are managed via Homeport rule sets and predefined roles/qualifiers. The rules and exceptions are documented in Homeport's system documentation and requirements.

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. The Privacy Act, 5 U.S.C.552a(m)(1) states that contractors maintaining a system of records on behalf of a Government agency shall be considered employees of that agency.

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

Yes.

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

Policy is in place and used by system approvers to ensure only those persons who should have access to the system are approved. The policy and procedures are documented in Guidelines for use of Port Security Functions Within Homeport Version 1.0, MPS Policy Letter 01-05.

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

Applications for access are reviewed and approved or disapproved by designated Coast Guard personnel.

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

Audits are conducted annually to validate access. Users that do not access the system for 90 days are deactivated. The system tracks data access for review, audit and/or disciplinary action.

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

Homeport provides users a web-based environment to view, share, and store appropriate maritime security information. The web-site contains a Homeport Users Guide and an in-depth Help section to assist in system negotiation. Coast Guard personnel accessing Homeport are required to have periodic training in the use of Sensitive But Unclassified information in addition to basic system operation instruction. Annual Privacy Act training is provided to Coast Guard Headquarters personnel who will access the system.

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

Yes. However, final C & A is pending approval of the Authority to Operate which is currently in routing. System is operating under an Interim Authority to Operate, which was signed on 20 April, 2006.

8.9 Privacy Impact Analysis

Access is restricted to specific users based on their profile so that they only will have access to that information they are allowed to access.

Section 9.0 Technology

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

System was built using a combination of commercial off the shelf software and government design software.

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

Data integrity and security were the primary considerations for the system.

9.3 What design choices were made to enhance privacy?

User accounts, access restrictions, and encrypted data transmissions were built in to ensure data integrity, privacy and security.

Conclusion

Account and access security was evaluated in order to ensure controlled and powerful personalization and customization software functionality, as such; the system has various user access levels to mitigate privacy risks. USCG Security Officials follow the same policy and guidelines for approving accounts and determining access groups. Homeport users must opt-in to share their profile information with other users.

USCG has designed a system that will ensure that only those individuals with a need to know have access to the lists of union personnel authorized to access their facility will be made available.

Responsible Officials

U. S. Coast Guard Privacy Officer, Mr. Donald Taylor, Address: Commandant (CG-611), U. S. Coast Guard, 2100 2nd Street SW, Washington, DC 20593-0001.

Project Manager, Commandant (G-PRI), U. S. Coast Guard, 2100 2nd Street SW, Washington, DC 20593-0001. Department of Homeland Security.