Privacy Impact Assessment Update

for the

Homeport Internet Portal

DHS/USCG/PIA-001(c)

June 19, 2017

Contact Point

Gary Chappell (CG-633)
United States Coast Guard
(202) 372-1280

Reviewing Official

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), United States Coast Guard (USCG) developed Homeport Internet Portal to serve as an enterprise tool that facilitates compliance with the requirements set forth in the Maritime Transportation Security Act (MTSA) of 2002, by providing secure information dissemination, advanced collaboration for Area Maritime Security Committees (AMSC), electronic submission and approval for facility security plans, and complex electronic notification capabilities. The collection of personally identifiable information (PII) concerning those with access to the Homeport system allows the USCG to validate the suitability and identify the eligibility of those who request permission or have access to the system. The USCG is conducting this Privacy Impact Assessment (PIA) update to: identify the new platform leveraged for information sharing, describe the separation of restricted and unrestricted data, and address the removal of the Alert and Warning System (AWS) functionality from Homeport.

Introduction

Background

The Maritime Transportation Security Act (MTSA)[1] established 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 sea ports. The Department of Homeland Security (DHS)/United States Coast Guard (USCG) is the lead federal agency for coordinating and implementing maritime homeland security and has significant enforcement responsibilities under the MTSA. Among its duties under the MTSA, the USCG requires maritime security plans be developed by the maritime private sector industry for ports, vessels, and facilities, and that those individuals with access to maritime facilities have credentials demonstrating their eligibility for such access.

Homeport Internet Portal collects registration information from representatives of the maritime industry; members of Area Maritime Security Committees; other entities regulated by the MTSA and USCG; as well as other users associated with a vessel, facility, or specific committee.[2] This tool serves as an enterprise portal combining secure information dissemination, advanced collaboration, and provides a public-facing interface for USCG processes. The main function of the Homeport Internet Portal is to facilitate online reporting and confirmation by facility owners and operators that their maritime facilities have attained the

[1] Pub. L. 107-295, *available at* https://www.gpo.gov/fdsys/pkg/PLAW-107publ295/pdf/PLAW-107publ295.pdf.
[2] Vessel and facility security officers (maritime industry personnel) need access to Homeport to submit and review vessel and facility security plans.

requisite security level in the event of a Maritime Security (MARSEC)[3] level change. Additionally, Homeport: 1) provides a secure method for the submission and storage of security plans by members of the maritime industry; 2) provides a secure capability for facility operators to view lists of personnel authorized to access their facility; 3) facilitates the secure submission of personal information by representatives of the maritime domain to the Transportation Security Administration (TSA) in order to conduct background screening and credentialing; and 4) provides a secure process for merchant mariner licensing and documentation applicants to ascertain the status of their credential application.

In 2009, a commercial-off-the-shelf (COTS) product was added to Homeport to retire the Government-developed custom software for MARSEC notifications. This COTS product, called the Alert Warning System (AWS), is an unclassified messaging mass notification system designed to broadcast and track notifications to specific individuals or groups.

In June 2011, in an effort to comply with Executive Order 13011, *Federal Information Technology*,[4] which seeks to improve Executive Branch agencies internal management of information system investments, USCG and TSA signed a Memorandum of Agreement (MOA) to allow the two organizations to share Homeport's AWS capabilities, consequently leveraging DHS's investment in the system and avoiding duplicate operations and maintenance costs within the Department.

In 2012, the Coast Guard Office of Strategy and Human Resources Capability, Commandant (CG-1B) sponsored AWS integration with the Navy Space and Naval Warfare Systems Command (SPAWAR)-managed CG Personnel Accountability Assessment System (CG-PAAS) to provide alert notifications and track personnel status. In 2013, Commandant (CG-1B) and the Coast Guard Office of Command, Control, Communications, Computers, and Sensor Capabilities, Commandant (CG-761) entered a joint sponsorship agreement to deploy AWS for USCG units to send routine and emergency alerts and warnings to USCG personnel. These new requirements drove the expansion of AWS far beyond the scope of the Homeport sponsor's original MARSEC requirements. During the 2013 Homeport system accreditation process, it became apparent that AWS was serving more functions than the original MARSEC notification functions it served in Homeport and therefore should be a separate system to accommodate the expanded system functionality and user community. A separate Federal Information Security Modernization Act (FISMA)[5] ID was requested for AWS and its system accreditation was

[3] Additional information on Maritime Security (MARSEC) levels and the change process for those levels is available in 33 CFR Part 101, *available at* https://www.gpo.gov/fdsys/pkg/CFR-2009-title33-vol1/pdf/CFR-2009-title33-vol1-part101.pdf.

[4] 3 CFR Part 13011, *available at* https://www.gpo.gov/fdsys/pkg/CFR-1997-title3-vol1/pdf/CFR-1997-title3-vol1-eo13011.pdf.

[5] Information regarding the Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. 113-283, is *available at* https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

achieved in early 2014. The AWS application and data are maintained as a separate information system, which is physically hosted, managed, and maintained by the USCG Operations Systems Center (OSC) in Kearneysville, WV. As a result, AWS is no longer part of Homeport.

Reason for the PIA Update

In order for the Homeport Internet Portal to meet the Department of Defense (DoD) cyber security mandates, USCG was required to upgrade the system and to replace obsolete software. USCG is replacing the current BroadVision content management system, which is at its end-of-life and is no longer supported by the vendor. The new content management system will be Microsoft SharePoint 2013. Functionality of the system will be similar; although the user interface may be somewhat different and additional capabilities associated with the SharePoint software will be available. DoD also requires physical separation of restricted and unrestricted data. The system upgrade will separate publicly available (unrestricted) information from restricted information, which is only available to logged-in users, in order to achieve compliance with this DoD mandate.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

Homeport will use SharePoint 2013 as its information sharing platform. Though the platform is changing, there is no new data being collected or displayed. All data associated with the AWS functionality introduced in the November 16, 2012, PIA update has been removed and moved to the separate AWS system.[6] The remaining data is covered under the original PIA and its subsequent updates.

Homeport is separated into two segments as follows:

1. Information items that are only accessible to authenticated users, and stored on a server residing within the Restricted Zone, and
2. Information items publicly accessible and stored on a server in the Unrestricted Zone.

1) Data stored in Non-Public/User-Authenticated Homeport (Restricted)

a) User Registration Process:

For representatives of the maritime domain, members of Area Maritime Security Committees, and other entities regulated by the MTSA that require an account to use

[6] *See* DHS/ALL/PIA-006 DHS General Contacts List, *available at* www.dhs.gov/privacy.

the Homeport portal, the following information will be collected through its online registration process. Initial collection for non-USCG users is performed through the "Unrestricted" (public-facing) Homeport site. The data collected is encrypted and saved as a JavaScript Object Notation (JSON)[7] file. The completed file is sent to the Unrestricted space on the Internet, and temporarily resides there. It is then retrieved and pulled into the Restricted (non-public) space.[8] This process occurs to facilitate the transmission of the file from an applicant who creates and completes the document outside of the USCG network. The following information is collected in the form:

Data Obtained from the General Public: (Items denoted with an asterisk are required form fields).

- First name;*
- Middle initial;
- Last name;*
- Company name;
- Business/work address*
- City;*
- State;*
- ZIP;*
- Work phone;*
- Mobile phone;
- 24-hour contact phone (*e.g.*, watch center or 24-hour facility);
- Fax;
- Pager;
- Email address;*
- Alternate email address;

[7] A JavaScript Object Notation (JSON) file is an open-standard format that uses human-readable text to transmit data objects consisting of attribute-value pairs.

[8] Unrestricted environment means that the encrypted file is temporarily stored in a space accessible to anyone on the Internet. However, the file retention in that space will only be for the duration of the polling frequency, which is planned for five seconds and the file cannot be read if accessed because it is encrypted. This method of moving these files from a member of the public to the Restricted (non-public) environment is required to prevent attacks on the IT system.

- Coast Guard Captain of the Port (COTP) zone;[9]
- Role in maritime industry;
- Vessels associated with the user;
- Facility role;
- Facilities associated with user; and
- Referral name/phone/email address.

Direct Access[10] data obtained from the Coast Guard Business Intelligence (CGBI) Enterprise Data Warehouse[11] (for Coast Guard civilian and military personnel):

- Employee ID;
- Department ID;
- Parent Department ID;
- Unit name;
- Administrative Target Unit (ATU);
- Operating Facilities (OPFAC);
- Operating Facilities Modifier (OPFACMOD);
- Job code;
- Job title;
- BCN;[12]
- Member type;
- Series rate;
- Grade level;
- Position Number;
- Position description;

[9] The area within which a Coast Guard Captain of the Port may exercise authority, as identified in 33 CFR Part 3, *available at* https://www.gpo.gov/fdsys/pkg/CFR-2016-title33-vol1/pdf/CFR-2016-title33-vol1-part3.pdf.

[10] *See* DHS/USCG/PIA-024 Direct Access, *available at* www.dhs.gov/privacy.

[11] *See* DHS/USCG/PIA-018 Coast Guard Business Intelligence (CGBI), *available at* www.dhs.gov/privacy.

[12] BCN is the Billet Control Number, a number assigned by the Coast Guard to uniquely identify each military position assigned to a Coast Guard unit. Position Control Numbers are used to uniquely identify civilian positions.

- USCG status;
- Rank;
- Employee class;
- Rotation date;
- Mobile phone; and
- Home phone.

USCG Active Directory Data Obtained from the CGBI Enterprise Data Warehouse (for Coast Guard Common Access Card (CAC) users:

- Work phone;
- Work email address;
- Fax; and
- Pager.

b) Transportation Worker Identification Card (TWIC) New Hire:

To fulfill the requirements of 33 CFR Part 105.257 and 33 CFR Part 104.267, Homeport collects and retains data from general public users (with a Homeport user account) that need to verify a newly-hired transportation worker's TWIC status. The data is captured from the logged-in and authenticated user on the Restricted Server and stored in the Restricted (non-public) database. It is used to perform a "live" query of the TSA TWIC database to obtain the status of a TWIC application, and return the query results to the authenticated user who generated the initial query. If the user passes the screening, and returns a passed TWIC status, he or she can begin immediate supervised access to his or her facility or vessel. Otherwise Homeport will continue querying TSA each night to see if a status has changed. If the status of the application changes, the submitter will be notified via email and can log into Homeport for more information. Once logged-in, his or her "My Homeport" tab will show the status of each of his or her active TWIC submissions.

Data Collected from the Public Logged-in User:

- Name;
- Date of birth; and
- Social Security number (SSN).

Data Displayed (returned in the query) to Logged-in User (Public and Coast Guard):

- Name;
- Date of birth; and
- SSN.

c) Mariner Training and Assessment Data:

Provides Mariner Training Centers and Schools a method for submitting course completion data sent to the Merchant Mariner Licensing Documentation (MMLD)[13] system in real-time using the USCG Enterprise Service Bus.[14]

Data transmitted in real time (not stored in Homeport):

- SSN.

Data collected/stored in Homeport:

- Last four digits of SSN.

d) Marine Events:

If an individual decides to complete a paper request, Homeport collects the information that is required on the Application for Marine Events[15] (CG-4423). The form must be completed in its entirety; users will not have the option to save the form and complete it at a later time. No additional identifying information will be collected or maintained by Homeport. The following Waterways Management Program data elements will reside temporarily in the Unrestricted database until retrieved and stored in the Restricted (non-public) database.

Data Collected from the Public:

- Name of event;
- Event date;

[13] *See* DHS/USCG/PIA-015 Merchant Mariner Licensing and Documentation System (MMLDS), *available at* www.dhs.gov/privacy.

[14] The Coast Guard Enterprise Service Bus (ESB) is an IT system that passes data between Coast Guard systems as standard XML services.

[15] A marine event is an organized event of limited duration held on the water according to a prearranged schedule. A marine event includes "any concentration of traffic on water, craft or not, participant or spectator, of a competitive or non-competitive nature, which is organized, limited in duration, conducted according to a prearranged schedule, and which would interfere with ordinary Navigation Rules in such a way as to require supplementary regulation." Any individual or organization (the sponsor) planning an event that by its nature, circumstances, or location, will restrict navigation or otherwise introduce extra or unusual hazards to the safety of life on navigable waters of the United States, is required by regulation to submit an application to the Coast Guard for review and approval. The receipt and review of the permit applications, and issuance or denial of the permits may be performed by the district office or delegated by the District Commander to a sector or unit.

- Time;
- Sponsoring organization name;
- Sponsor address;
- Number of vessels/craft/swimmers;
- Sizes of participating boats/craft;
- Types of participating boats/craft;
- Number of spectator craft;
- Description of event;
- Will this event interfere of impede the natural flow of traffic;
- What extra or unusual hazard (to participants or non-participants) will be introduced into the regatta area;
- Have any state/local authorities, stakeholders, or interested parties objected to the proposed event, vessels, and/or other support provided by sponsoring organization for safety purposes;
- Does the sponsoring organization deem its patrol adequate for safety purposes;
- Is a Coast Guard Patrol Asset requested;
- "Person in charge" name;
- How can the "person in charge" be contacted during the event? Be specific and provide number and or channel;
- Where will "person in charge" be during the event;
- "Person in charge" address;
- "Person in charge" phone;
- Email address; and
- Captain of the Port (COTP) zone.

e) Security Plans:

This application allows Port Partners to submit security plans, TWIC addendums, Shipboard Security Alert System (SSAS) documents, and other supporting documents in Homeport. The submitted documents and other data are passed directly over to Marine

Information for Safety and Law Enforcement (MISLE) system[16] via the Operation Systems Center's (OSC)[17] Enterprise Service Bus. Several security measures have been put in place, including the use of a Lightweight Directory Access Protocol (LDAP)[18] server in CGOne, to ensure this did not create security concerns for MISLE. Homeport interacts with the LDAP server also by using the Enterprise Service Bus. It must keep all user credential and demographic data up to date so MISLE can use the LDAP service to validate user requests. Users submit vessel and facility plans for vessels and facilities they associated with themselves when registering for their account. These vessels and facilities are loaded and updated each night using an extract from MISLE, which is the system of record for vessels and facilities. Once a plan is submitted, the approvers are notified of the submission via an email generated by Homeport. The approvers can then log into MISLE to begin working on the plan. All status changes are communicated back to Homeport via a direct database link. Status changes are then processed and users are notified of them. When logging in, users can view status changes, past history, and the plan itself, if approved. Users also have the ability to add other users as viewers of plans that they have submitted. All of these data requests occur in real time from MISLE to Homeport. For security reasons, Homeport does not store any of this information. Rather, it uses the Enterprise Service Bus to query MISLE in real time for the data.

f) Port Status:

This application was created during the Deepwater Horizon Oil Spill to facilitate smooth commerce by keeping Port Partners informed of local port statuses. Statuses include open, closed, or open with restrictions. Each status can contain notes about the status to provide more information. Only USCG users have the ability to modify existing ports in their COTP zone. No personally identifiable information is collected from the public.

g) Maritime Security (MARSEC):

This application disseminates the National as well as local COTP zone MARSEC levels. The National MARSEC level is pulled directly from the USCG's primary Internet page and will change accordingly if the level changes. USCG users at each COTP zone, who are given a certain publishing access group, have the ability to modify the MARSEC

[16] *See* DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE), *available at* www.dhs.gov/privacy.

[17] The United States Coast Guard Operations Systems Center (OSC) is a government-owned, contractor-operated facility with the primary function of providing full life-cycle support for operationally-focused Coast Guard automated information systems

[18] The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. LDAP provides a central place to store usernames and passwords which allows different applications and services to connect to the LDAP server to validate users.

level for their COTP zone. No personally identifiable information is collected from the public.

h) <u>People Search</u>:

Homeport allows CAC-authenticated Homeport users (may be USCG civilian, military, or contractor) to search for information about other CAC-authenticated Homeport users. The data that is searched is stored in Restricted Homeport.

Direct Access Data Obtained from the CGBI Enterprise Data Warehouse (for Coast Guard Civilian and Military Personnel):

- Name;
- Company;
- Work address line 1;
- Work address line 2;
- Work city, work state;
- Work ZIP code;
- Work country;
- Cell phone;
- Secondary email address;
- 24-Hour contact phone (*e.g.*, watch center or 24-hour facility);
- Work phone;
- Fax;
- Pager; and
- Work email.

Data obtained from Homeport Restricted Database:

- Last Login;
- COTP zone;
- Other COTP zones;
- Vessel roles;
- Vessels;

- Facility roles;
- Facilities;
- Harbor Safety Committee (yes/no);
- Safety Advisory Committee (yes/no);
- Port Readiness Committee (yes/no);
- Third Party Vessel Response Plan (VRP) Submitter (yes/no);
- VRP company name;
- Community memberships;
- Publishing Master; and
- Non-disclosure form.

2) Data Stored in Publicly Accessible Homeport (Unrestricted)

a) <u>Merchant Mariner Application Status</u>:

Merchant Mariners are able to check the status of their application for Merchant Mariner certificates online. Users must enter at least two of the three italicized data elements listed under "MMLD Data Obtained from the CGBI Enterprise Data Warehouse." The query retrieves the application and all certificates associated with the application. The user will see the status of his or her application and the statuses of any of the certificates. The user is also able to click on the certificate to see a further clarification of the status. For example, some certificates may be in "awaiting testing" status, and any tests the user needs to take will be listed.

MMLD Data Obtained from the CGBI Enterprise Data Warehouse:

- *Reference Number;*[19]
- *Application ID;*
- *Last Name;*
- Application status;
- Date received;
- Regional Exam Center address;

[19] Italicized data elements are used to uniquely identify the record in MMLD so that the correct information is provided in response to the request.

- Credential;
- Transaction type;
- Credential state/status;
- Credential status date; and
- Status information:
    - Standard verbiage that applies to the particular status. For example, if the status is ISSUED, the verbiage states the date it was mailed, days to allow for delivery, and National Maritime Center (NMC) contact information if the credential is not received within the expected timeframe.

Data Displayed to the Public (Anonymous User):

- Reference Number (if used as the search criteria);
- Last name (if used as the search criteria);
- Application ID;
- Application status;
- Date received;
- Regional Exam Center address;
- Credential;
- Transaction type;
- Credential state / status;
- Credential status date; and
- Status information:
    - Standard verbiage that applies to the particular status. For example, if the status is ISSUED, the verbiage states the date it was mailed, days to allow for delivery and NMC contact information if the credential is not received within the expected timeframe.

b) Merchant Mariner Credential Verification and Merchant Mariner Certificate:

Both of these functions use the same data and query parameters. Merchant Mariner Credential Verification allows a public (non-logged in) user to verify the authenticity Merchant Mariner certificates. The user can check Merchant Mariners individually or in groups, or he or she can check by a specific document. Users must enter some combination of the italicized data elements listed under "MMLD Data Obtained from the CGBI Enterprise Data Warehouse." The application then pulls back the list of certifications matching those criteria. The user can then click on each individual certificate to see a list of the capacities, limitations, and regulations attached to that certificate. The user can also print out the information in a PDF. The application allows a Merchant Mariner to select and print his or her Merchant Mariner Certificate to display for personal use.

MMLD Data Obtained from the CGBI Enterprise Data Warehouse:

- First name;
- Last name;
- Middle name/initial;
- Suffix;
- Reference Number;
- Citizenship;
- Gender;
- Credential type;
- Credential Number;
- Credential issue date;
- Credential expiration;
- Document Number;
- Document type; and
- Credential information:
    - Serial Number;
    - Reference Number;
    - Issue date;
    - Expiration date;
    - Capacities; and
    - Limitations.

Data Displayed to the Public (Anonymous User):

- First name;
- Last name;
- Middle name/initial;
- Suffix;
- Reference Number;
- Citizenship;
- Gender;
- Credential type;
- Credential Number;
- Credential issue date;
- Credential expiration;
- Document Number;
- Document type; and
- Credential information:
    - Serial Number;
    - Reference Number;
    - Issue date;
    - Expiration date;
    - Capacities; and
    - Limitations.

c) Merchant Mariner Credential Survey:

This application allows users to provide feedback on the USCG National Maritime Center credentialing process. Feedback will be used to guide the NMC's efforts to improve its services and processes. No personally identifiable information will be collected.

d) Merchant Mariner Sea Service Calculator:

This application allows Merchant Mariners to determine if they met the sea service requirements for renewing their Master, Mate, Engineer, Pilot, Operator Uninspected Passenger Vessel (OUPV), and MMD credentials. No personally identifiable information will be collected.

e) Vessel Response Plans (VRP) Express:

VRP Express allows public users to query metadata associated with a Vessel Response Plan.

Data Obtained from the MISLE Database/Displayed to the Public (Anonymous User):

- Basic Search Menu
    - Allows the user to search for every vessel in VRP Express by either Vessel Name or Plan Number
- Advanced Search Menu
    - Allows the user to sort by multiple categories at once, as well as by categories that basic search does not allow, such as:
        - Type of cargo/fuel carried;
        - Vessels traveling to specific COTP zones;
        - Qualified individual company name;
        - Specific qualified individuals;
        - Name of company providing Oil Spill Removal Organization (OSRO) service;
        - Which vessels have a Remote Zone Contract (Actual Contract not Accessible);
        - Which vessels have a specific Navigational Restriction on their approval letter;
        - Name of company providing System Management and Engineering Facility (SMEF) services;
        - Name of company providing aerial observation and dispersant resources; and
        - Which vessels are under specific flags.
- Vessel Search
    - Shows every vessel in VRP Express and is sortable by the following categories:

    - Vessel Name;
    - International Maritime Organization (IMO)/Official Number;
    - Authorization status of the vessel;
    - Plan Number;
    - Plan expiration date;
    - Vessel's worst case discharge;
    - Vessel's tonnage; and
    - Vessel type.

- Plan Number Search
  - Shows every plan in VRP Express sortable by the following categories:
    - Plan Number;
    - Plan holder (Owner/Operator) company name;
    - Plan preparer company name;
    - Authorization status of the Plan;
    - Plan expiration date; and
    - Plan type (tank/NT(Non-Tank Vessel)/IMO/combination).
- Plan Details Page
  - Shows details about a plan including the following:
    - Plan holder (Owner/Operator) point of contact, company name, and address (phone, fax);
    - Plan preparer point of contact, company name, and address (phone, fax); and
    - Plan type, highest Worst Case Discharge (WCD), and approval and expiration dates.
  - A list of the vessels in the Plan with the following information:
    - Vessel name and IMO/Official Number;
    - Vessel authorization status;
    - Vessel and Plan type;
    - Vessel's WCD; and

        - Link to Vessel Approval Letter.
- Vessel Details Page;
    - Shows details about a specific vessel including the following:
        - Vessel's IMO/Official Number, type of Plan, and vessel's WCD;
        - Vessel owner's name and operator's name;
        - Vessel's flag and call sign;
        - Type of vessel and type of cargo carried; and
        - Largest oil tank, length of vessel, and tonnage.
    - A list of COTP Zones the vessel calls with the following information:
        - Zone name and vessel's authorization status in zone; and
        - Any navigational restrictions, alternate planning criteria, or lightering restrictions.
- General Service Administration (GSA) Information Page
    - Shows the following information about a specific vessel within a specific COTP zone:
        - Qualified individuals' names and company names;
        - Names of companies providing OSRO, aerial observation, dispersant resources, salvage services, and firefighting Services; and
        - Any alternate planning criteria, navigational restrictions, lightering arrangements, and in which operating areas the vessel is authorized.
- Vessel Approval Letter
    - Shows the following information:
        - USCG VRP staff address, phone, fax, and email;
        - Plan holder (owner/operator) company name, point of contact, and address;
        - Plan preparer company name, point of contact, and address;
        - Vessel name and IMO/Official Number;
        - List of approved COTP zones and navigational restrictions; and

- USCG point of contact's signature.

Uses of the System and the Information

The uses associated with the AWS functionality introduced in the November 16, 2012, PIA update have been removed. There are no other uses of information changes to the Homeport system.

Retention

In accordance with National Archives and Records Administration's (NARA) disposition authority number N1-026-06-06, records of registration information are destroyed upon account termination. Maritime personnel screening data is destroyed after two years. Response-associated information, such as personal data needed for search and rescue purposes, is destroyed 120 days following completion of response operations.

Internal Sharing and Disclosure

Homeport collects data from CGBI on Coast Guard military and civilian personnel to verify their identity as Homeport users. Information collected includes: name, work address, email address, and phone number. This information is only available to system administrators. However the names of users are available to all registered users to find other users through a search function.

Homeport shares data with MISLE for the purpose of submitting and viewing facility and vessel security plans. Security plans are submitted by facility and vessel security officers who are authorized Homeport users for review and approval by the Coast Guard. They can also submit updates to those plans using the same process. Facility and vessel security officers can view the documents they submitted using Homeport; however, the data for those plans are retained in MISLE. Facility and vessel security plans include contact information for personnel involved in implementing those plans, including: name, work address, work phone, and work email.

Homeport shares data with MMLD for the purpose of pushing Mariner Training and Assessment Data (MTAD) entered into Homeport to MMLD. Once the data is received by MMLD, it is no longer retained in Homeport. MTAD data includes the name and mariner number for Merchant Mariners that have taken courses at educational institutions approved by the Coast Guard, along with information on courses they have taken and certifications completed. Homeport receives data from MMLD for the Mariner Application Status function.

Data received includes: name, mariner number, application number, and application status. This data is not displayed to users but is used for record matching. When mariners enter their identification data into Homeport, they receive their application status. That same data is used for the Mariner Credential Status function, which verifies that a mariner has a valid credential.

Homeport receives data from the TSA Infrastructure Modernization (TIM) system for the purpose of implementing the TWIC New Hire provision. Data includes the worker's name, SSN, date of birth, and TWIC application status. This data is not provided to users but is used for record matching by the system. Employers enter a worker's name, SSN, and date of birth into Homeport to determine the worker's TWIC processing status. This allows a worker to have access to a vessel of facility prior to obtaining his or her TWIC card. Once a TWIC card is issued or his or her application is denied, the data is deleted from Homeport.

External Sharing and Disclosure

The names of qualified individuals responsible for executing response plans and the point of contact for the plan preparer are made available to the public on Homeport. This information is needed by personnel responding to a spill to avoid delays in responding to the spill. These personnel are notified of this disclosure by their employer when response plans are submitted to the Coast Guard.

Homeport no longer shares lists of union personnel authorized to access their facility. This function was replaced when the TWIC program became operational and is to some extent replaced by the TWIC New Hire function in Homeport discussed in the TIM entry above.

Privacy Risk: There is a privacy risk in displaying the names of qualified individuals and the point of contact for the plan preparer to members of the public.

Mitigation: This risk is not mitigated. 33 CFR Part 155.1026 requires that the qualified individual and the alternate qualified must be available on a 24-hour basis. Most response personnel do not have access to restricted Homeport data. Therefore, first responders to a spill require the name of the qualified individual since they are responsible for executing the spill response plan. The present configuration does not permit this risk to be further mitigated.

Notice

Notice of the collection of information by the Homeport Internet Portal is provided to individuals via the publication of this PIA update, as well through a Privacy Act Statement posted on the system's collection screen. Additional notice is provided through DHS/USCG-

060 Homeport SORN.[20]

Privacy Risk: There is a privacy risk that individuals may not be aware that their information is being collected, maintained, and displayed by the Coast Guard within the Homeport system.

Mitigation: This risk is mitigated through the publication of this PIA update, as well as through the Privacy Act Statement posted on the collection screen within the system. Additional notice was provided through the publication of the Privacy Act System of Record Notice, DHS/USCG-060 Homeport, in the Federal Register (79 FR 74747). The system is configured so that users may decide whether or not their information is displayed on Homeport. Registered users may grant or decline consent to other registered users to view their information through the Preference Option available in Homeport. Access to the information is mitigated by only allowing users with authorized access to view certain information. Additionally, vessel owners, operators, and qualified individuals consented to the release of their contact information on Homeport at the time the Vessel Response Plan was submitted.

Individual Access, Redress, and Correction

Individuals are able to access their data through their system profile. Individuals, regardless of immigration status, may also request access to their records under the Freedom of Information Act (FOIA). Additionally, U.S. persons may request access under the Privacy Act. Individuals may also file a privacy complaint with the DHS Privacy Office. Individuals seeking to correct erroneous information, regardless of immigration status, may submit a request to correct data to the following address:

Department of Homeland Security
United States Coast Guard Headquarters
Commandant (CG-633)
2703 Martin Luther King Jr. Ave. SE
Washington, D.C. 20593-0001

Technical Access and Security

The technical access and security remains consistent with Section 8.0 of the May 9, 2006, Homeport PIA in which authorized users, managers, system administrators, and developers all have access to the system. 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

[20] *See* DHS/USCG-060 Homeport, 79 FR 74747 (December 16, 2014).

and requirements.

Technology

Homeport Internet Portal will be upgraded to SharePoint, a web application platform in the Microsoft Office server suite that facilitates information sharing.

Responsible Official

LCDR Don Hunley
CG-633
United States Coast Guard

Marilyn Scott-Perez
Privacy Officer (CG-61)
United States Coast Guard

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security