Privacy Impact Assessment Update
for the

Homeport Internet Portal

DHS/USCG/PIA-001(b)

November 16, 2012

Contact Point
CDR Ted Kim
U.S. Coast Guard
(202) 372-1278

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) currently uses the Homeport Internet Portal to provide secure information dissemination, advanced collaboration for Area Maritime Security Committees (AMSC), electronic submission and approval for facility security plans, and complex electronic notification capabilities. Homeport includes a subsystem called the Alert Warning System (AWS), which provides USCG Headquarters, Districts, Sectors, and other units an enterprise solution for sending alerts and warnings to maritime security (MARSEC) partners, stakeholders, and appropriate port constituents for MARSEC level changes and other MARSEC-related activities requiring port-wide notifications. Through a Memorandum of Agreement (MOA) between the USCG and the Transportation Security Administration (TSA), use of AWS capabilities will be shared between these two DHS components, thereby leveraging DHS investment in the system and avoiding duplicative operations and maintenance costs within DHS. The USCG is issuing this Privacy Impact Assessment (PIA) update to include TSA operations center personnel as authorized users of Homeport's AWS, which contains non-sensitive personally identifiable information (PII) and disseminates airport security information to authorized recipients.

Introduction

Background

The Maritime Transportation Security Act (MTSA) of 2002 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 ports. The DHS/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 that maritime security plans be developed by 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, which collects registration information from 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, has an existing system of records notice (SORN) under the Privacy Act of 1974 and an existing PIA.[1] This tool serves as an enterprise portal that combines secure information dissemination, advanced collaboration, and provides a public-facing interface for USCG processes.

TSA protects the nation's transportation systems to ensure freedom of movement for people and commerce. With state, local, and regional partners, TSA oversees security for highways, railroads, buses, mass transit systems, pipelines, and ports. With the bulk of their

[1] The DHS/USCG-060 Homeport SORN and DHS/USCG/PIA-001 Homeport Internet Portal PIA may be found at www.dhs.gov/privacy.

efforts in aviation security, TSA is solely responsible for screening passengers, and checked and carry-on baggage at 450 U.S. airports.

In June 2011, and consistent with Executive Order 13011, *Federal Information Technology*, which purpose is in part to improve executive agencies internal management of information systems investments, an MOA between USCG and TSA was signed to share Homeport's AWS capabilities, consequently leveraging DHS investment in the system, and avoiding duplicative operations and maintenance costs within DHS.

Reason for the PIA Update

This PIA update is based on the implementation of a database in Homeport for TSA's alert recipients, which include TSA personnel and aviation partners/stakeholders. As a service provider under the MOA, USCG will provide full system operations and administration support to include the configuration of an AWS Virtual Private System (VPS) instance for TSA's use that provides the delivery of alerts to multiple pagers, mobile phones, e-mail addresses, home phones, work phones, or faxes for a single end user. The VPS also has the capability to send Simple Mail Transfer Protocol (SMTP) and Short Message Service (SMS) to TSA designated recipients.

Functionally, there are two separate, distinct application interfaces, the USCG AWS and the TSA AWS. These applications and respective data are isolated from each other. USCG administrators use USCG AWS to send alerts to USCG personnel. Authorized TSA users will use TSA AWS to send alerts to their counterparts. In other words, only authorized users at TSA's operational centers will access the TSA portion of the system to send out alerts to TSA personnel and aviation partners and stakeholders, as well as receive replies from the aviation recipients. Furthermore, while the user information of both USCG and TSA personnel are stored in an encrypted Homeport database server, the actual data are stored in separate, secure USCG-specific or TSA-specific files. TSA provides USCG with sufficient funding for system lifecycle support.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

Contact information for TSA's use in the AWS will be collected from a variety of sources, depending on the identity of the alert recipients, and will be provided to the USCG Homeport system administrators who will create the TSA AWS database contact list. Alert recipients include non-TSA personnel such as airport police officers, airline security personnel, and airport authority personnel. Other non-TSA personnel may include officials from other government agencies and businesses in the various transportation sectors. Alert recipients voluntarily provide information directly to TSA so that TSA can notify them in the event of an emergency or transportation-related security incident. The PII collected will consist of a person's name, email address, and phone number(s).

Uses of the System and the Information

AWS provides TSA offices and airports with an enterprise solution to expeditiously and simultaneously send out alerts and warnings to aviation security partners, stakeholders, and

appropriate aviation personnel for aviation security-related activities, such as airport police officers, airline security personnel, and airport authority personnel. Such personnel, who may be external to TSA, may voluntarily provide contact information to TSA so that TSA can store that information in AWS and notify them in the event of an emergency or transportation-related security incident. Recipients of the alerts and warnings benefit with increased awareness of airport activities, allowing for appropriate response action planning if necessary.

Retention

All identifying information used to send alerts and notifications will be overwritten each time the data provider enters new information via a service registry function.

Internal Sharing and Disclosure

Internal sharing and disclosure of information have not changed with this PIA update. Internal sharing and disclosure will be in accordance with the previous Homeport PIA and PIA updates, the provisions of the Privacy Act, 5 U.S.C. § 552a, and routine uses in the DHS/USCG-060 Homeport System of Records Notice (SORN).[2]

External Sharing and Disclosure

The only information that AWS shares with external aviation security and law enforcement partners is the content of the alerts that are sent. If there is a need for sharing information, all external sharing of PII is compatible with the original collection of information and covered by the DHS/TSA-008 Notification Contact Lists SORN.[3]

The potential privacy risks of improper external sharing are mitigated by having an appropriate SORN in place for AWS that identifies routine uses by which external sharing may occur. TSA data incorporated into the Homeport system of records may be shared externally consistent with the routine uses defined in applicable the DHS/USCG-060 Homeport SORN.

Notice

Notice is provided to individuals via this PIA update and a Privacy Act Statement. In addition, notice related to TSA AWS users is provided in the DHS/TSA-008 Notification Contact Lists SORN.

Individual Access, Redress, and Correction

Individual access, redress and correction have not changed with this PIA update. Individuals are able to access their data through their system profile. Individuals seeking to correct erroneous information may submit a request to correct data to the following address:

Department of Homeland Security
United States Coast Guard Headquarters

[2] The DHS/USCG-060 Homeport SORN (November 9, 2009, 74 FR 57692) may be found at http://www.dhs.gov/system-records-notices-sorns.
[3] The DHS/TSA-008 Notification Contact Lists SORN (December 10, 2004, 69 FR 71828) may be found at http://www.dhs.gov/system-records-notices-sorns.

Commandant (CG-633)
2100 2nd Street, S.W.
Washington, D.C. 20593-0001

The guideline will be posted in the Privacy Statement on the Homeport TSA AWS website.

Technical Access and Security

Technical access and security risks remain unchanged by the addition of TSA users of AWS.

Technology

The technology employed by Homeport remains unchanged by the addition of TSA users of AWS.

Responsible Official

CDR Ted Kim
U.S. Coast Guard
202-372-1278
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

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