Privacy Impact Assessment Update
for the

U.S. Coast Guard
"Biometrics At Sea"

DHS/USCG/PIA-002(c)

July 12, 2011

Contact Point
CDR Pat DiBari
USCG C2 and Information Systems
United States Coast Guard
(202) 372-2483

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Coast Guard (USCG), a component of the Department of Homeland Security (DHS) and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program partnered to provide mobile biometrics collection and analysis capability at sea using the "Biometrics At Sea" system, along with other remote areas where DHS operates. USCG published its Biometrics At Sea (BASS) Privacy Impact Assessment (PIA) DHS/USCG/PIA-002(b) March 14, 2008 and can be viewed at http://www.dhs.gov/files/publications/gc_1281126129297.shtm. DHS is updating the 2008 PIA in order to incorporate the USCG maritime mobile biometrics system use of Universal Serial Bus (USB) cable and encrypted hard drive instead of the encrypted flash drive to facilitate the air gap transfer of biometric and biographic data from the system laptop to the onboard computer that is connected to the USCG Data Network Plus.

Introduction

This USCG Maritime BASS PIA Update focuses on a change in the technology used in the air gap transfer of biometric and biographic data from the system laptop to the onboard computer. USB flash drives have been shown to have inherent security issues when mounted to computer systems and were subsequently prohibited on USCG information systems in 2008. The USCG maritime mobile biometrics system now uses the USB cable and encrypted hard drive instead of the flash drive to facilitate the air gap transfer of biometric and biographic data from the system laptop to the onboard computer that is connected to the Coast Guard Data Network Plus (CGDN+). Encrypted USB cables and hard drives do not demonstrate security problems associated with most flash drives. With this mandated change in technology, the resulting biometrics system is more secure, and the potential risk to privacy is reduced. USCG and US-VISIT incorporate the collected biometric information (digital fingerprints, photograph), plus limited biographical information, into IDENT as well as gain access to and communicate with other biometric databases accessible through arrangements between IDENT and other national and international agencies.[1]

Participating Coast Guard cutters are capable of transmitting biometric data (digital fingerprints, photograph) via efficient, secure, and encrypted means to US-VISIT for comparison against the IDENT database and DHS-accessed databases. Following successful receipt of each biometric record, US-VISIT compares the biometric information against the IDENT and DHS accessed databases and communicates a "Hit" or "No Match" response to the Coast Guard. Relevant criminal history information is available to Coast Guard and DHS decision makers to consider with respect to disposition of interdicted persons (e.g., repatriation, referral for prosecution, etc.).

---

[1] Visit DHS/USCG/PIA-002(b) "Biometrics at Sea"at http://www.dhs.gov/files/publications/gc_1281126129297.shtm and DHS/USVISIT-0012 DHS Automated Biometric Identification System (IDENT) at http://edocket.access.gpo.gov/2007/07-2781.htm for additional information.

As fully described in the March 14, 2008 PIA regarding maritime mobile biometric use with interdicted migrants, the Coast Guard retains no biometric data from the initial collection at sea after submission to and successful enrollment in the IDENT database or other applicable database. All such data are deleted, erased, and/or destroyed after the Coast Guard:

1. Verifies receipt and enrollment by US-VISIT or other applicable database;
2. Repatriates the migrants or transfers them to U.S. authorities ashore for prosecution, as material witnesses in a prosecution, or for other processing in accordance with pre-existing approved immigration or other procedures; and
3. Completes the Coast Guard cutter patrol (typically 3-5 days).

The USCG does not maintain its own biometric database.

The USCG uses maritime biometrics for law enforcement (LE) activities; primarily for Alien Migrant Interdiction Operations (AMIO), but also to support other LE/Maritime Homeland Security (MHLS) operations.

This PIA update recognizes a general use of maritime biometrics by the USCG as it improves data transfer technology to all areas of USCG operations.

Reason for the PIA Update

The USCG is submitting this update to the PIA for its maritime mobile biometrics system for the following reason:

The USCG has forbidden the use of flash drive technologies due to the system security weaknesses they impose. The USCG maritime mobile biometrics system now uses an encrypted USB cable and hard drive instead of the encrypted flash drive to facilitate the air gap transfer of biometric and biographic data from the system laptop to the onboard computer that is connected to the Coast Guard Data Network Plus (CGDN+). There are no other technical or privacy updates to this PIA.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

This update only changes the technology used as part of the system and not the information collected.

Uses of the System and the Information

No additional privacy risks are associated with this update. Identification is required of those entering the U.S. for commerce and other lawful activities.

Retention

Retention schedules are unchanged by the updates:

All biometric data collected at sea is enrolled into IDENT to become a part of its permanent database. After the information is uploaded to IDENT and confirmed to the USCG, the collected information is subsequently deleted from the stand-alone, non-networked system. The USCG does not permanently maintain any database with this biometric data.

Per existing guidance regarding IDENT, records in IDENT are retained until the statute of limitations has expired for all criminal violations or the records are older than 75 years. The biometric information collected will only be retained in IDENT and not by the USCG. Associated biographical data may be retained in accordance with existing federal information laws and policies.

Internal Sharing and Disclosure

There are no changes to internal sharing and disclosure with this update. The PIA states:

The system itself shares no data. USCG will collect data on undocumented aliens and other suspected criminals and enroll them into IDENT. The USCG information obtained will only be uploaded and shared in accordance with USCG and DHS policies that govern the use of data. This information may be shared with CBP, ICE, TSA, USCIS, and others as defined by the IDENT SORN, which includes USCG and DHS policies in effect. The sharing of this information will continue to comply with the IDENT PIA and SORN.

External Sharing and Disclosure

There are no changes to external sharing and disclosure with this update. The PIA states:

Any external sharing of the information collected will be through IDENT. IDENT has information sharing arrangements with other external organizations, including DOS and DOJ. The USCG use of IDENT data or content and its submission of data for enrollment in IDENT does not alter DHS information sharing arrangements with external organizations.

US-VISIT on behalf of USCG will share biometrics (digital fingerprints and digital photograph) and biographic information (name, gender, date of birth, nationality, if available, and disposition) for national security, law enforcement, immigration, intelligence, and other DHS mission-related functions that require the use of biometrics to identify or verify the identity of individuals. The USCG has consented to US-VISIT sharing

information supplied for inclusion in the recidivist portion of IDENT that identifies repeat offenders on immigration laws with any appropriate party per these terms. The sharing of this information will continue to comply with the IDENT PIA and SORN.

Notice

Notice procedures will remain the same as in the PIA:

Notice is provided by means of this PIA through publication on the DHS website. The USCG, other DHS component agencies, and other government agencies will jointly publicize information regarding the collection of biometrics by the USCG. In addition, USCG personnel will distribute to all persons interdicted at sea copies of a standard notification of biometrics collection, including a description of the uses of biometric information and contact information for redress.

Individual Access, Redress, and Correction

There are no changes to access, redress, and corrections with this update. No changes to privacy risks have occurred.

Technical Access and Security

The USCG maritime mobile biometrics system now uses the USB cable and encrypted hard drive instead of the flash drive to facilitate the air gap transfer of biometric and biographic data from the system laptop to the onboard computer that is connected to the Coast Guard Data Network Plus (CGDN+). Encrypted USB cables and hard drives do not display security problems associated with most flash drives. With this mandated change in technology, the resulting biometrics system is more secure, and the potential risk to privacy is reduced.

Only authorized USCG personnel (including contractors) who require access to the equipment and data used in the USCG collection of biometric data in the performance of their duties will have access to this equipment and information. Such personnel may include crew members on board USCG vessels that are equipped with the biometric equipment discussed above and Command Center or other personnel who may be required to transmit information to, from or between USCG vessels and US-VISIT/IDENT in the performance of their duties. As set forth above, any media containing biometric/IDENT data (including the laptops and external media) used by the USCG to collect biometric data will be stored in approved security containers when not in use to which only approved personnel will have access.

Technology

USB flash drives have been shown to have inherent security issues when mounted to computer systems and were subsequently forbidden on USCG information systems. The USCG maritime mobile biometrics system now uses an encrypted USB cable and hard drive instead of the flash drive to facilitate the air gap transfer of biometric and biographic data from the system laptop to the onboard computer that is connected to the Coast Guard Data Network Plus (CGDN+). Encrypted USB hard drives do not display security problems inherent to most flash drives. With this mandated change in technology, the resulting

biometrics system is more secure, and the potential risk to privacy is reduced. Under the Authority to Operate, the security of the USCG maritime biometrics system is tested through required security scans every 180 days. These security tests, along with policy, procedures, and training, provide insurance that the privacy risks are mitigated with this biometric technology.

Responsible Official

CDR Pat DiBari
USCG C2 and Information Systems
United States Coast Guard
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security