Privacy Impact Assessment Update
for the

Biometrics at Sea System (BASS)

DHS/USCG/PIA-002(d)

December 6, 2016

Contact Point
CDR Kristi Bernstein
Office of Law Enforcement (CG-MLE-2)
United States Coast Guard
(202) 372-2166

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

Abstract

As the United States' primary maritime law enforcement agency, the U.S. Coast Guard (USCG) enforces United States immigration statutes and regulations at ports, at sea, and around the world. USCG implemented the Biometrics At Sea System (BASS) on 23 of its cutters in the District 7 Area of Responsibility (AOR)[1] to screen individuals attempting to enter the United States illegally via maritime routes. USCG uses BASS to collect and send biometric information to DHS's Automated Biometric Identification System (IDENT), a repository of biometric and associated biographic data used for, among other purposes, national security, law enforcement, and immigration and border management. USCG is updating this Privacy Impact Assessment (PIA) to modernize its biometric submission and response architecture and to mitigate risks associated with the processes to expand the collection, use, and maintenance of biometrics collected from individuals interdicted by the Coast Guard.

Overview

The Coast Guard conducts patrols and coordinates with other federal agencies and foreign countries to interdict individuals at sea, suspected of or engaged in illicit smuggling activities. In the course of operations, USCG encounters individuals of unknown identity, some of whom may be known or suspected terrorists, linked to trans-national criminal syndicates, aggravated felons, or individuals previously interdicted for suspected illicit activity.

Federal law requires that USCG conduct a program for the mobile identification of individuals in the maritime environment.[2] To continue meeting this requirement, and the recent goals associated with DHS and USCG initiatives to degrade illicit networks operating in the maritime environment, the USCG intends to expand BASS into known maritime threat vectors within the Western Hemisphere Transit Zones (WHTZ) to collect and send biometric information to DHS's Automated Biometric Identification System (IDENT),[3] which shares that information with the Department of Justice's (DOJ) Next Generation Identification system

[1] District 7 is based in Miami, Florida, and covers Sectors Charleston, Jacksonville, Key West, Miami, San Juan, and St. Petersburg. USCG cutters in District 7 typically interdict individuals in the Mona Pass (area between the Dominican Republic and Puerto Rico), and the surrounding south Florida waters.
[2] 46 U.S.C. § 70123.
[3] For an extensive discussion of the privacy risks and mitigations surrounding the IDENT database, *please see* DHS/NPPD/PIA-002 Automated Biometric Identification System PIA (December 7, 2012), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system. The Office of Biometric Identity Management (OBIM), formerly US-VISIT, manages IDENT. IDENT stores and processes biometric data—digital fingerprints, photographs, iris scans, and facial images—and links biometrics with biographic information to establish and verify identities. On behalf of USCG, OBIM shares biometrics information with authorized users for national security, law enforcement, immigration, intelligence, and other DHS mission-related functions that require its use to identify or verify the identity of individuals.

(NGI)[4] and the Department of Defense's (DoD) Automated Biometric Identification System (ABIS)[5].

Biometrics at Sea Background

DHS conducted two comprehensive PIAs for the BASS program in 2006 and 2008, respectively. DHS is now updating the BASS PIA in full to provide a more accurate description of USCG as the data steward and responsible data owner for biometrics collected as part of the BASS program – including coverage under a USCG system of records notice; describe new sharing arrangements with the Department of Justice and the Department of Defense; update the type of mobile biometric capture technology employed by USCG in the field; and assess any privacy risks noted in the 2015 Office of the Inspector General (OIG) report regarding BASS.

The USCG at-sea biometric capability was originally deployed in 2008 to meet four goals. First, it provides the foundation to develop DHS mobile biometric capabilities. Second, it provides decision makers with information to assist in the determination of courses of action in USCG law enforcement interdictions; (e.g., repatriate, arrest, refer for prosecution), by providing additional identifying information of interdicted persons not available without at-sea biometrics collection and analysis. Third, it deters human smuggling networks by improving enforcement of U.S. immigration laws.[6] The USCG maritime biometrics system enables the USCG and federal prosecutors to identify repeat offenders of immigration laws and other persons of law enforcement interest who are frequently interdicted at sea. It also enhances the ability to identify smugglers and persons involved in smuggling networks. Finally, the USCG maritime biometrics system can help preserve life at sea because of increased deterrence to the inherently dangerous and illegal trade of human smuggling. USCG experience demonstrates as prosecutions increase, fewer undocumented aliens attempt the dangerous and illegal passage to the United States via maritime means.[7]

---

[4] Integrated Automated Fingerprint Identification System/Next Generation Identification Biometric Interoperability, *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis-ngi-biometric-interoperability.

[5] Automated Biometric Identification System (ABIS), *available at* http://ciog6.army.mil/Portals/1/PIA/2015/DoD%20ABIS.pdf.

[6] Including, without limitation, 8 U.S.C. § 1324 (bringing in and harboring aliens), 1325 (improper entry by alien), 1326 (reentry of removed aliens) and 1327 (aiding and assisting aliens to enter).

[7] As described in the original 2006 and 2008 PIAs for BASS, the BASS Proof of Concept program in Mona Pass (the area between the east coast of the Dominican Republic and the west coast of Puerto Rico) commenced on November 17, 2006. As of November 14, 2007, the Coast Guard obtained biometrics from 1364 undocumented migrants interdicted in the Mona Pass. 289 of those were identified in the IDENT database. To date, persons interdicted in the Mona Pass and identified in the IDENT database include convicted felons (including persons convicted of violent crimes, drug trafficking and gang related offenses), recidivist immigration violators, and numerous persons subject to final orders of deportation. Information obtained through biometrics analysis assisted the U.S. Attorney's Office in San Juan to commence 93 new prosecutions for violations of U.S. immigration law between November 17, 2006 and November 14, 2007. During this period, migrant flow across the Mona Pass

Scope of USCG biometric collections

The USCG Biometrics at Sea program does not intentionally capture biometrics from U.S. citizens. Through the at-sea screening process of citizenship documentation, USCG collects biometric information only from appropriate individuals who are the focus of law enforcement efforts.[8] The USCG does not collect biometric information from any individual providing appropriate documentation to verify his or her status within the United States unless there are reasonable grounds to suspect such documents may be fraudulent or due to exigent circumstances in which immediate identification is needed for purposes of criminal investigation of an offense for which such person is reasonably suspected or for purposes of officer safety. Persons presenting facially valid documents evidencing status in the United States are processed in accordance with pre-existing approved procedures for interdiction and entry into the United States;[9] U.S. citizens are either returned to their vessel to continue their voyage or are transported to the next U.S. port at which the USCG vessel stops for processing in accordance with U.S. Customs and Border Protection (CBP) policies and procedures. If subsequent to collection of biographic information a person is found to be a U.S. citizen, his or her biometric data is deleted and not shared.

Participating Coast Guard cutters are capable of transmitting biometric data (digital fingerprints and photograph) via efficient, secure, and encrypted means to be enrolled in the IDENT database.[10]

Biometrics at Sea Collection Process

BASS consists of a portable handheld device to capture fingerprints, a laptop, and an encrypted hard drive. The BASS process works as follows:

During Alien and Migrant Interdiction Operations (AMIO),[11] authorized personnel on board a USCG cutter issue a numbered armband to the intercepted alien under custody. This

---

decreased by at least 40%; an unprecedented reduction in illegal activity in this vector.

[8] *See id.*

[9] *See* 33 CFR part 160.

[10] In a biometric security system, enrollment refers to the initial process of collecting biometric data samples from a person and subsequently storing the data in a reference template representing an individual's identity that the organization uses later for comparison against other biometric data.

[11] As the primary maritime law enforcement agency, the Coast Guard is tasked with enforcing immigration law at sea. The Coast Guard conducts patrols and coordinates with other federal agencies and foreign countries to interdict undocumented migrants at sea, denying them entry via maritime routes to the United States, its territories, and possessions. Interdicting migrants at sea means they can be quickly returned to their countries of origin without the costly processes required if they successfully enter the United States. The Coast Guard supports the National Policy to promote safe, legal, and orderly migration. Illegal immigration can cost U.S. taxpayers billions of dollars each year in social services. In addition to relieving this financial burden on our citizens, the Coast Guard's efforts help to support the use of legal migration systems. Primarily, the Coast Guard maintains its humanitarian responsibility to prevent the loss of life at sea, since the majority of migrant vessels are dangerously overloaded, unseaworthy, or otherwise unsafe.

armband, which the alien is required to wear while in custody, serves as the main identifier linking the alien to the captured biometrics and biographic information (name, date of birth, sex, and nationality). Authorized personnel record the biographic information in an AMIO log.

Authorized personnel use the handheld device to collect fingerprints and capture a facial image of aliens the USCG intercepted during AMIO. The handheld device has built-in algorithms to recognize whether a fingerprint meets acceptable handheld device standards, i.e., is a good print. If the fingerprint does not meet standards, the handheld device prompts USCG personnel to retake the print. If the second fingerprint is not acceptable, a third is required.

USCG personnel download captured biometrics to a dedicated laptop and enter biographic information. A laptop formats the data and exports the records to an encrypted external hard drive. USCG personnel transfer the biometric and biographic information to a USCG networked workstation and then by encrypted email, securely, to IDENT.

IDENT automatically compares the biometrics received from USCG against existing biometrics within the IDENT database and sends a match or no match response to the appropriate USCG Command Center—a shore-based operational unit that supports and coordinates cutter operations. This response serves as a confirmation from IDENT that it has received and compared the biometric information against existing information in its database. When there is no match, IDENT enrolls the new biometrics in its database.

In the event IDENT encounters an issue with the captured biometrics, IDENT automatically sends the issue to the USCG Command Center and the BASS system support agent at the Command, Control, and Communications Engineering Center (C3CEN) to resolve the issue. The Command Center may instruct personnel on the cutter to retake the fingerprint if necessary to complete the identification and enrollment process.

Depending on the result of the IDENT match, the USCG Command Center instructs cutter personnel to detain the alien for prosecution, repatriate the alien, or take other appropriate actions.

Biometric and biographic information from BASS is stored in IDENT. USCG clears all biometric data from the handheld devices, encrypted hard drives, and networked workstations once IDENT receives and acknowledges the results.

DHS Office of Biometric Identity Management as a Service Provider

DHS Office of Biometric Identity Management (OBIM) is the DHS biometric service provider for the Department. OBIM operates the information technology system, IDENT, as the DHS biometric repository shared IT service.[12] Consistent with the DHS Privacy Policy

[12] DHS/NPPD/PIA-002 Automated Biometric Identification System PIA (December 7, 2012), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system, at page 2.

Memoranda for the Roles & Responsibilities for Shared IT Services (June 11, 2011)[13], all uses of data through IDENT shall be compatible with the purpose for which that data was originally collected by DHS and all uses shall comply with all applicable privacy compliance requirements, including all data retention and use limitation requirements of the original data steward – in this case, USCG. As a service provider, OBIM provides a service to its data stewards and data users. OBIM identifies each collection by data steward (in this case, USCG) and its authority to use, retain, and share it. IDENT enables sharing of BASS information with authorized users only after USCG has approved the sharing. IDENT stores and processes biometric data—digital fingerprints, photographs, iris scans, and facial images—and links biometrics with biographic information to establish and verify identities. OBIM operates IDENT as a biometric repository service to DHS components, such as USCG, to enable data providers to retain control over their own information.

Pursuant to the Shared IT Services policy referenced above, USCG is the data steward for all biometrics collected by the BASS program and stored in IDENT. USCG maintains the following responsibilities for BASS information within IDENT:

a) Document the legal authority and the purpose for the collection and use of the data.

b) Document criteria for the appropriate use of data through IDENT.

c) Document that IDENT includes sufficient controls to enable the Coast Guard to validate the use of the data, including managed access.

d) Ensure that all additional uses of the data are legally authorized, appropriate, and compatible with the purpose for which the data was originally collected.

e) Ensure and document that the data is maintained according to DHS and National Archives and Records Administration (NARA) approved records retention schedule. If a records retention schedule is not yet approved, ensure that all data is maintained until a records retention schedule is approved. This is the USCG's responsibility even though IDENT physically stores and manages the data.

f) Complete all privacy compliance requirements for the data including a System of Records Notice.

g) Publish the data in the DHS Data Asset Repository.

h) Ensure that all IDENT users of BASS complete all privacy compliance requirements prior to using the data received from IDENT.

[13] DHS Privacy Policy Memoranda 2011-02 Roles & Responsibilities for Shared IT Services (June 11, 2011), also identified as DHS Policy Directive 262-09, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2011-02.pdf.

i) Approve and document uses of the data through IDENT.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The USCG's collection of biometric information is in support of its law enforcement and other missions as authorized by 14 U.S.C. §§ 2 (U.S. Coast Guard Primary Duties), 89 (U.S. Coast Guard Law Enforcement); and 19 U.S.C. §§ 482 (Search of vehicles and persons), 1401(i) (Officer of the customs; customs officer).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/USCG-031 USCG Law Enforcement (ULE) SORN, which DHS is publishing concurrent with this PIA covers the collection and use of BASS data.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

In May 2015, the DHS OIG determined that USCG was several years out of compliance regarding a System Security Plan for BASS.[14] The DHS OIG recommended that USCG update the BASS Security Plan, Security Impact Analysis, and Interface Control Agreement, including ensuring that security controls are consistent with appropriate security requirements. The DHS Privacy Office concurs with this recommendation.

The USCG completed the Security Impact Analysis, updated the Interface control agreement, and updated the System Security Plan (SSP) for BASS as recommended by the DHS OIG. The latest SSP update was completed on December 29, 2015. The Authority to Operate is pending completion of this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Previously, USCG relied upon the IDENT records retention period for biometrics stored in IDENT. As described above, as a Component Data Steward, USCG is responsible for managing its own records retention requirements for biometrics collected by USCG and sent to

[14] *See* "The Security Posture of the United States Coast Guard's Biometrics At Sea System Needs Improvements," DHS Office of the Inspector General Report OIG-15-41 (March 3, 2016), *available at* https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-41_Mar15.pdf.

IDENT.

Biometric records must be held in accordance with the applicable system of records notice and records retention schedule. USCG is publishing a new SORN to provide coverage for its biometric collections and will work with NARA to establish a records schedule consistent with its SORN coverage.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The collection of biometric and related biographic information from persons crossing the border is covered by OMB Control Number 1651-0138, which is assigned to DHS/CBP.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The USCG collects biometric data from persons who are interdicted at sea or as a result of at-sea interdictions reasonably suspected of violations of U.S. law, international treaty, or convention. Authorized USCG personnel will obtain biometric data from such persons while performing duties within the scope of their authority under U.S. and international law. The USCG will not collect biometrics from individuals who provide appropriate documentation to verify a legal nexus or citizenship status within the United States unless a) there are reasonable grounds to suspect such documents may be fraudulent; b) because of exigent circumstances, immediate identification is needed for purposes of a criminal investigation of an offense for which such person is reasonably suspected; or c) for purposes of officer safety.

Typically, the USCG collects biometric information from the following individuals:

1. Undocumented aliens who are attempting to enter or re-enter the United States in violation of U.S. law; (AMIO)
2. Persons reasonably suspected of migrant smuggling in violation of U.S. law; (AMIO)
3. Other persons interdicted at sea in connection with AMIO; (AMIO)
4. Persons reasonably suspected of maritime drug trafficking; (AMIO or PSO)

5. Persons reasonably suspected of terrorist activity or support of terrorist activity in violation of U.S. or international law;[15] (AMIO or PSO)
6. Confirmation of crew identity in security boardings[16] or other suspected violations of U.S. laws with respect to vessel master and crew nationality on vessels in U.S.waters; (PSO)
7. Identification of persons in Search and Rescue operations; (AMIO/PSO)
8. Persons who are reasonably suspected of violating security/safety zones and/or threatening maritime commerce and/or transportation in violation of U.S. law. (PSO)

The interdicted persons provide the limited biographic information about themselves in connection with the USCG's routine processing. This may include statements, identifying documentation, or both. USCG will share biometrics (digital fingerprints and digital photograph and biographic information (name, gender, date of birth, nationality, if available).

Interoperability

DHS OBIM; USCG; the Department of Defense (DoD) Biometrics Identity Management Agency (BIMA); and the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division have developed an interim submission architecture to support DHS/USCG activities to enhance the use of mobile biometric identification of suspected individuals, including terrorists, in the maritime environment. The DHS/USCG will use the USCG Biometric at Sea System to provide real-time submission and response in the Western Hemisphere Transit Zone (WHTZ) as needed and approved by the commanding officer of the vessel in accordance with USCG policy guidelines.

Real-time submission and response will allow DHS/USCG to search individual biometrics against OBIM's IDENT database, the DOD ABIS database, and DOJ's NGI. Prior to this update, the biometric information USCG collected consisted of 10 print and a facial image submitted via USB cables and encrypted hard drives for file-handling and transfer to the Coast Guard's Data Network (CGDN to IDENT).

This update provides for submission of biometric data through approved Secure File Transfer Protocol (SFTP) connectivity utilizing the Joint Special Operations Command (JSOC), Mobile Operations Biometric Software (MOBS) collection and transmission software build. As

[15] Including activity defined or described in 18 U.S.C. § 2331-2332f, 2339, 2339A-C.
[16] A security boarding is an examination by an armed boarding team of a vessel (including the cargo, documentation and persons onboard), arriving at, departing from, or operating in a U.S. port, to deter and prevent acts of terrorism and/or transportation security incidents, destruction, loss, or injury from sabotage or other subversive acts. Guidance on the conduct of security boardings is contained in the U.S. Coast Guard Maritime Law Enforcement Manual (MLEM), COMDTINST M16247.1(series).

discussed here, transmitting biometrics from BASS through this improved process allows the submission process to reduce the steps previously taken for submission and provide real-time submission and response directly from and to the Crossmatch® Secure Electronic Enrollment Kit (SEEK) device independent of the Coast Guard Data Network (CGDN).

2.2 What are the sources of the information and how is the information collected for the project?

The USCG collects biometric data directly from persons reasonably suspected of violations of U.S. law who are interdicted at sea or as a result of at-sea interdictions.

BASS also includes responses from IDENT after submission. IDENT automatically compares the biometrics received from USCG against existing biometrics within the IDENT database and sends a match or no match response. This response serves as a confirmation from IDENT that it has received and compared the biometric information against existing information in its database. When there is no match, IDENT enrolls the new biometrics in its database.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

USCG trained personnel capture biometric data (digital fingerprints and photographs) with mobile devices l directly from the individual, which ensures a high degree of accuracy. The portable system incorporates real-time quality checks to ensure the quality of fingerprints captured is sufficient for enrollment in IDENT. Additionally, C3CEN conducts regularly recurring reviews of IDENT quality scores for USCG enrollments to determine that the USCG is providing sufficient quality images.

The interdicted persons provide the limited biographic information about themselves in connection with the USCG's routine processing. This may include statements, identifying documentation, or both. Therefore, the biographic information is as accurate as the statements and documentation that the individuals provide.

When downloading information from mobile devices to the stand-alone non-networked computer, confirmation is provided that the information has been downloaded and subsequently deleted from the handheld. Information uploaded into IDENT will not be completely deleted from all parts of the stand-alone system until there is confirmation that the records have been successfully enrolled in IDENT.

Ownerships and Reconciliation Gaps

During the course of its 2015 audit, the DHS OIG found considerable discrepancies in the number of biometrics submitted to IDENT from BASS. The USCG failed to maintain an accurate accounting of biometric disclosures from BASS to IDENT. From the OIG report:

> USCG did not implement a regular reconciliation process because there was confusion as to the owner of the biometrics information sent from the cutters. At the beginning of this audit, USCG officials stated that they did not own the biometrics captured, and had no further responsibility after the biometric information left the cutters. Subsequent to our additional discussions with OBIM officials, USCG officials acknowledged ownership of the data.[17]

This PIA further reiterates that the USCG, as the Component Data Steward under the DHS Shared IT Services policy,[18] is the data owner for all biometrics submitted to IDENT from BASS and is responsible for the accuracy, timeliness, and correctness of all information collected via BASS.

Mobile Capture Device Upgrade

In response to recommendations from the DHS OIG that the USCG "establish a BASS aggregate control log to verify biometric transactions from the 23 cutters, and perform periodic reconciliation with IDENT,"[19] the USCG now uses paper logs to document BASS transactions. This provides data for a comparative analysis with similar metrics maintained by IDENT to ensure the absence of or identify any possible transmission gaps.

To ensure reconciliation with IDENT, the USCG will conduct a six-month proof of concept technology demonstrator designed to test the Crossmatch® Secure Electronic Enrollment Kit (SEEK) device for real-time biometric submission and response screening of individuals encountered at sea. The SEEK 2 device stores transactions in an internal log; however, reconciliation current Standard Operating Procedure (SOP) is to delete the internal transaction logs after use. Biometrics transfer transactions are currently completed manually through comparison between IDENT Transactions and Command Center response logs. A process to modernize the control log reconciliation process is in progress.

---

[17] *See* "The Security Posture of the United States Coast Guard's Biometrics At Sea System Needs Improvements," DHS Office of the Inspector General Report OIG-15-41 (March 3, 2016), *available at* https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-41_Mar15.pdf.

[18] DHS Privacy Policy Memoranda 2011-02 Roles & Responsibilities for Shared IT Services (June 11, 2011), also identified as DHS Policy Directive 262-09, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2011-02.pdf.

[19] *See id.*

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of inaccurate data due to manual data entry throughout the adjudication process.

Mitigation: This risk is partially mitigated. Training is provided to BASS users and a Standard Operating Procedure has been established to guide users in proper data entry. Periodic checks of BASS data entry are performed by C3CEN in accordance with the BASS Quality Assurance Surveillance Plan (QASP). The QASP requires verification that data is properly entered and associated with the correct individual.

Privacy Risk: There is a risk of mis-association between the biometric and biographic data being collected during separate portions of the intake process.

Mitigation: This risk is partially mitigated. Training is provided to BASS users and a Standard Operating Procedure has been established to guide users in proper data collection and entry. Periodic checks of BASS data entry are performed by C3CEN in accordance with the BASS QASP. The QASP requires verification that data entered at different points in the intake process is associated with the correct individual.

Privacy Risk: There is a risk that USPER data will be collected for migrant enforcement or immigration and shared as such.

Mitigation: USCG personnel use documents to verify the citizenship of persons prior to collection of data and have been trained to detect fraudulent or altered documents. In the event that documentation is not available, subsequent investigation using the collected biometrics is used to establish identity and citizenship. If after collection of biometric information an individual is determined to be a U.S. citizen, his or her biometric information is deleted and not shared.

Privacy Risk: There is a risk that not all data collected on board the USCG Cutters may be accounted for in IDENT.

Mitigation: Not all data collected on board USCG Cutters is intended to be accounted for in IDENT. The USCG uses transaction logs, response receipts from IDENT, and periodic checks of BASS data entry by C3CEN to ensure that data intended for retention in IDENT is sent to and retained by that system.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The USCG will use biometrics for identity verification to determine if individuals interdicted at sea have been previously encountered and their biometrics enrolled in IDENT. Following successful receipt of each biometric record, IDENT compares the biometric information against the full IDENT gallery of previously enrolled biometrics 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 the disposition of interdicted persons (e.g., repatriation, referral for prosecution).

Based on this information the USCG will determine, in coordination with other DHS agencies, if these persons pose a threat to the boarding teams or to national security, are wanted for any criminal offenses, or have an immigration history including prior deportation or removal from the United States. Of particular concern to the USCG are persons identified as known or suspected terrorists, aggravated felons, previous deportees (i.e., felons or other persons who have received a final order of deportation from the United States) and recidivist violators of U.S. immigration laws (i.e., persons with multiple prior removals from the United States). Such information is critical in informing decisions by the USCG, DHS, and DOJ to detain, arrest, or prosecute such persons for violations of U.S. law.

As described in the November 3, 2006 PIA, 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:

- Verifies receipt and enrollment by IDENT,
- 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,
- Completes the Coast Guard cutter patrol (typically 3-5 days).

While the primary uses of BASS are for law enforcement (LE) activities, such as for Alien Migrant Interdiction Operations (AMIO), USCG may also use biometrics capabilities to support other maritime homeland security (MHLS) operations such as crewmen identity verification or screening aboard certain vessels entering U.S. Ports as a condition of entry.

Alien Migrant Interdiction Operations (AMIO)

The USCG's alien maritime interdiction operations (AMIO) are directed to the unsafe

transportation of migrants by sea that include all vessels not properly manned, equipped, or licensed for carrying passengers on international voyages. The vast majority of people that the USCG interdicts at sea in connection with AMIO are not U.S. citizens and are attempting to illegally enter the U.S. Such individuals, at a minimum, violate 8 U.S.C. § 1325 (improper entry by an alien). Human smuggling violates numerous federal laws and places the migrants' lives at risk. The ability to identify persons previously deported or removed from the U.S. is critical to the USCG's fulfillment of its Law Enforcement, national, and Humanitarian and Life Saving missions. Persons who have been previously deported or removed and attempt to re-enter the U.S. violate federal law, including 8 U.S.C. §§ 1325, 1326. The use of at-sea biometrics capabilities enables the USCG to identify persons who violate these or other immigration laws, as well as persons who are wanted for other crimes or are on a known or suspected terrorist watch list.

Port Security Operations (PSO)

The USCG's Captain of the Port Authority may deem certain cargo vessels entering U.S. Ports as a higher risk based on security and safety protocol vetting conducted on each vessel. As a result, vessels designated as a High Interest Vessel and/or vessels requiring a Condition of Entry security boarding may be subject to biometric screening to verify the identity of the crew as directed by the Captain of the Port. The use of biometric screening enables the USCG to confirm the identity of the crew as well as identify persons who are wanted for other crimes or are on a known or suspected terrorist watch list prior to entry into a U.S. Port.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. USCG sends all biometric and limited biographic information directly for search and enrollment in the IDENT system, owned and operated by OBIM. Other DHS components may search these USCG biometrics stored within IDENT, consistent with a need to know in performance of their official duties.

The two biometric feeds from USCG stored within OBIM are:

1. USCG Port Security Operations (identity verification of crew members arriving in or with access to U.S. ports)

2. USCG Alien Migrant Interdiction Operations

DHS Components that access these feeds are:

CBP uses the data for its trusted traveler programs to provide expedited transit for pre-approved, low-risk international travelers through dedicated U.S. border POEs. In the future CBP may use the data for its biometric exit program.

U.S. Immigration and Customs Enforcement (ICE) uses the data for investigations, or for processing arrests, bookings, detentions, and/or removals from the United States. ICE also uses the data as part of its overstay process.

U.S. Citizenship and Immigration Services (USCIS) uses the data to establish and verify the identities of individuals applying, and being adjudicated for immigration benefits, including asylum or refugee status.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk to use limitation because the USCG does not have a governance process in place to approve and manage uses of the biometrics at sea information.

Mitigation: The USCG has an MOU with OBIM regarding the handling of BASS data. That MOU limits sharing of information to "authorized DHS personnel who have a need to know to carry out their official duties." OBIM has a process to verify an individual's need to know when screening them for issuance of an account to access IDENT data. Additionally, the USCG SORN covering the collection of biometrics through BASS provides scoping for the use of BASS information through its purpose statement.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

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.[20]

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The USCG collects biometric data directly from persons reasonably suspected of violations of U.S. law who are interdicted at sea or as a result of at-sea interdictions. Due to the law enforcement nature of this information collection, individuals do not have an opportunity to consent or opt-out of this collection of information.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk associated with notice because all biometrics are collected directly from interdicted individuals by uniformed members of the USCG. Additionally, all such individuals receive a notice explaining the collection.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Under the previous BASS PIA, the USCG asserted that all data from the initial biometric collection at sea will be deleted and erased from a USCG standalone computer aboard each cutter upon confirmation of successful enrollment into the IDENT database and therefore not retained by the USCG. The USCG also asserted that all biometrics submitted from the USCG to IDENT are retained until the statute of limitations has expired for all criminal violations or the records are older than 75 years. This has not changed.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk to retention because the USCG does not have a records retention policy for BASS information within IDENT.

Mitigation: The USCG will retain all records in IDENT until a biometrics records retention schedule is approved by NARA. The USCG is actively pursuing a new schedule with NARA. The USCG expects that the NARA approved records schedule will be the same as the 75 year retention required for other IDENT records.

[20] See Attachment for an English language version of this notice.

Privacy Risk: There is a risk to retention because the USCG does regularly not audit whether the biometrics have been deleted off of the mobile capture devices or standalone computers.

Mitigation: BASS mobile devices are regularly examined for maintenance by the C3CEN staff. When the devices are examined, C3CEN staff verifies that all biometric data has been deleted. If the C3CEN staff identifies biometric data on the mobile device they delete that data during maintenance.

Privacy Risk: There is a risk to retention because IDENT has a retention period of 75 years for all biometrics, which does not permit component data stewards to exercise control over their information and their respective records schedules.

Mitigation: The USCG will retain all records in IDENT until a biometrics records retention schedule is approved by NARA. The USCG expects that the NARA approved records schedule will be the same as the 75 year retention required for other IDENT records. If NARA requires a different records retention schedule, the USCG will work with IDENT to arrange disposal in accordance with the NARA records schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

USCG currently shares biometrics (digital fingerprints and digital photograph) and biographic information (name, gender, date of birth, nationality, if available, and disposition) within DHS 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 under the "One DHS" information sharing initiative.

Any other external sharing of BASS is done through the search function within IDENT. However, as described above, the USCG is still responsible for:

a) Documenting criteria for the appropriate use of data through IDENT.

b) Documenting that IDENT includes sufficient controls to enable the Coast Guard to validate the use of the data, including managed access.

c) Ensuring that all additional uses of the data are legally authorized, appropriate, and

compatible with the purpose for which the data was originally collected.

These responsibilities extend to both internal and external uses of the biometrics and biographic information sent to IDENT from BASS.

The following external organizations access data collected by BASS through the IDENT system:

Department of Defense (DOD): uses the data to identify terrorists and individuals that present a national security threat. This use is authorized under the MOU between DOD and DHS on Information Sharing and Technology Partnering Relating to Identity Verification and Screening Activities and the DHS Information Sharing Strategy.

Department of Justice (DOJ): The FBI uses the data for law enforcement investigations. The Terrorist Screening Center uses the data to identify suspected terrorists. This use is in accordance with the DHS Information Sharing Strategy and the One DHS Information Sharing Memorandum.

Department of State (DOS): Uses the data when screening personnel for benefits. Also for screening employees and contractors. This use is in accordance with the DHS Information Sharing Strategy and the One DHS Information Sharing Memorandum.

INTERPOL and Foreign Government Law Enforcement Agencies use the data to identify terrorists. This use is in accordance with the DHS Information Sharing Strategy and the "One DHS" Information Sharing Memorandum.

Office of Personnel Management (OPM): OPM uses the data to screen employees and contractors prior to employment. This use is in accordance with the DHS Information Sharing Strategy and the One DHS Information Sharing Memorandum.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The DHS/USCG-013 ULE SORN includes in routine uses the sharing of information with law enforcement agencies. This applies to the disclosures to DOJ, INTERPOL, and foreign government law enforcement agencies. The SORN routine uses also include sharing with federal, state, or local agencies with which the U.S. Coast Guard has a Memorandum of Understanding or Memorandum of Agreement. This applies to DOD, DOS, and OPM. This sharing is compatible with the law enforcement reasons for which these records were collected.

6.3 Does the project place limitations on re-dissemination?

No. Until recently, the USCG relied solely on IDENT sharing arrangements to control the dissemination of USCG data. Data made available to DOJ/NGI and DoD/ABIS is limited to "search" only.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

USCG does not keep any record of BASS records disclosed outside of the Department; instead, USCG relies upon OBIM to retain an accounting of records disclosed outside of the Department as part of IDENT. The disclosures include records that are paper-based or electronic and record the date, nature, and purpose of each dissemination and disclosure, along with the name and address of the individual or agency to which the disclosure is made. This list of disclosures is retained as part of the accounting requirements for the IDENT system in order to be able to recreate the information to demonstrate compliance.

IDENT maintains an audit record in the database for each system message sent to an external agency. Audit logs are maintained by the IDENT Operations and Maintenance (O&M) Team and the Information Technology Management Branch. Access to audit logs is limited strictly to core O&M personnel. The audit log data is backed up regularly as part of the overall IDENT database backup and archiving process.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data shared by USCG with external partners will be used beyond the original purpose of collection (marine safety and security).

Mitigation: Biometric data shared with DOJ's NGI and DoD's ABIS is provided for screening purposes only in support of USCG enforcement of laws and treaties missions. The business rules in place are for "search only" and arise out of separate interoperability agreements between DHS and DOJ or DoD, respectively. Biometric data is retained by these agencies only as provided for in agreements between DHS and those agencies.

Privacy Risk: There is a risk that USCG does not have any governance regarding which external parties have access to BASS information within IDENT.

Mitigation: This risk is not mitigated. The Coast Guard has not documented its governance process with respect to access to BASS information within IDENT. The Coast Guard will develop and document a process for determining access to BASS information within IDENT and will work with OBIM to ensure that process is implemented.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The individual should submit a written request for the information that includes his or her name, mailing address, and if known, the date or dates on which the information was collected and, if also known, the name of the Coast Guard vessel on which it was collected, to the System Manager at the following address: Department of Homeland Security, United States Coast Guard, Commandant (CG-611), 2703 Martin L. King Jr. Avenue SE, STOP 7710, ATTN: FOIA Coordinator, Washington, D.C. 20593-7710. A request may also be submitted to EFOIA@uscg.mil.

The biometric and limited biographic information obtained from undocumented aliens or other persons that the USCG interdicts at sea may be exempt from individual access because access to the data in IDENT could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. Determinations will be made after evaluation of each request.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals should submit requests to contest or amend information as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access.

7.3 How does the project notify individuals about the procedures for correcting their information?

USCG notifies individuals of the procedures for correcting their information in this PIA and corresponding SORNs set forth in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that under the previous SORN structure, all BASS information was considered exempt for law enforcement purposes, thereby potentially denying redress to individuals whose information should not be exempt from access, correction, and amendment.

Mitigation: Access procedures are provided in this section. The determination as to whether information is exempt from access will be made on a case by case basis.

Privacy Risk: Under the USCG Law Enforcement (ULE) SORN, there is risk that redress may not be granted to persons from whom the biometrics are collected**.**

Mitigation: An individual may have an opportunity to correct his or her data when it is being collected; otherwise, he or she may submit a redress request directly to OBIM privacy officer who will coordinate with USCG on the response. If an individual is not satisfied with the response from OBIM/USCG, the individual may appeal his or her case to the DHS Chief Privacy Officer, who may conduct a review and provide final adjudication on the matter.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Only authorized USCG personnel (including contractors) who are required to collect, submit, receive, and/or assess biometrics and or biometric results in the performance of their duties will have access to this equipment and information.

As set forth above, any media containing biometric/IDENT data (including laptops and external media) used by the USCG to collect or assess biometric data will be stored in approved security containers or work spaces to which only approved personnel will have access when not in use.

USCG intends to use additional software capabilities for submitting biometrics to IDENT via expanded interoperability with DOD and DOJ biometrics databases, and receiving responses in near real-time during a six-month proof of concept in the WHTZ and subsequently in other USCG areas of responsibility as the program matures and expands.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All USCG personnel who access BASS equipment or IDENT data are trained using USCG and DHS-approved privacy training courses regarding the proper handling of personally identifiable information (PII) and proper use of the information systems to ensure the information is safeguarded. Special training is provided to BASS equipment users to ensure that PII is properly handled and deleted from the BASS equipment after use.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to BASS equipment and IDENT data is determined by USCG Maritime Law Enforcement (CG-MLE) policy and the unit Commanding Officer, who selects the personnel at the unit that will use and safeguard the BASS equipment. The same personnel will receive and handle any IDENT data returned when data submissions are sent to IDENT.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The USCG operates BASS under the provision of the One DHS Memo. At this time, the USCG does not review or approve any information sharing agreements, MOUs, or new uses of BASS information.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a risk that BASS information is not audited or accounted for in a manner required under the Privacy Act and internal DHS policy.

Mitigation: CG-MLE policy limits the personnel that will have access to BASS equipment and any information collected on that equipment and information received from IDENT. Personnel are given training on the use of BASS equipment and the handling of PII to ensure that PII is properly protected. Units now maintain logs of information submitted to IDENT to compare with IDENT records to ensure that USCG properly accounts for information. The BASS equipment is maintained by C3CEN personnel who, as a part of their maintenance, ensure that no PII is retained on BASS equipment.

Privacy Risk: There is a risk that USCG is unable to account for how BASS information

is shared, used, or accessed internal and external to DHS.

Mitigation: This risk is not mitigated. The Coast Guard has not documented its governance process with respect to access to BASS information within IDENT. The Coast Guard will document a process for determining access to BASS information within IDENT and will work with OBIM to ensure that process is implemented.

Responsible Officials

CDR Kristi Berstein
Office of Law Enforcement (CG-MLE-2)
United States Coast Guard
(202) 372-2166

Marilyn Scott-Perez
Chief Privacy Officer (CG-61)
United States Coast Guard
(202) 475-3515

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

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

ATTACHMENT

NOTICE

PERSONS CONTEMPLATING UNAUTHORIZED VOYAGES TO BRING MIGRANTS INTO THE UNITED STATES are cautioned that such actions may violate numerous U.S. civil and/or criminal laws and subject the individuals involved to ARREST, SEIZURE of any VESSELS utilized, heavy FINES and/or PENALTIES, and CONFINEMENT IN PRISON. Specific prohibitions include:

1. ASSISTING OR ATTEMPTING TO ASSIST A FOREIGN NATIONAL TO ENTER THE U.S. WITHOUT PRIOR PERMISSION (visa) FROM U.S. IMMIGRATION OFFICIALS (8 U.S.C. ßß 1321-1324) - vessel forfeiture, up to $100,000 fine and one year in prison for each alien, or up to $250,000 fine or five years in prison if done for financial gain. Higher penalties if anyone is injured or killed during the attempt.

2. ATTEMPTED ILLEGAL ENTRY or RE-ENTRY AFTER DEPORTATION (8 U.S.C. ß 1325-1326) - up to $100,000 fine, up to 20 years in prison (for attempted re-entry), or both.

3. FAILURE TO HEAVE TO (18 U.S.C. ß 2237) - criminal penalties to a master, operator, or person in charge of a vessel, who knowingly and intentionally fails to obey an order to heave to, impedes a boarding, or makes false statements regarding the vessel or voyage. A fine up to $10,000 or five years in prison, or both.

4. RESISTING OR IMPEDING U. S. LAW-ENFORCEMENT OFFICERS engaged in the performance of their duties (18 U.S.C. ß 111) - up to $250,000 fine and three years in prison.

5. NEGLIGENT AND GROSSLY NEGLIGENT OPERATIONS, INCLUDING OVERLOADING VESSELS OR FAILURE TO HAVE ADEQUATE SAFETY EQUIPMENT for the number of persons onboard (46 U.S.C. 2302 & 4308) - Civil penalty up to $27,500 and possible vessel forfeiture.

6. LOSS OF PAROLE, DETENTION, AND INITIATION OF REMOVAL PROCEEDINGS - Persons granted immigration parole and others who have legal status as immigrants in the U.S. face possible revocation of parole, detention, and initiation of removal proceedings.

7. TAMPERING WITH SEIZED PROPERTY (18 U.S.C. ß 2232) - up to $250,000 fine and five years in prison.

8. MAKING A FALSE OFFICIAL STATEMENT (18 U.S.C. ß ß1001, 2237) - up to $10,000 fine and five years in prison.

NOTICE REGARDING USE OF BIOMETRICS

1. U.S. law enforcement personnel, including the U.S. Coast Guard, will obtain biometric information from persons interdicted on vessels en route to the United States (including Puerto Rico and Mona Island). The information obtained will include digital fingerprints and photographs. This information will be used by law enforcement personnel in the enforcement of U.S. laws, including the laws described above, and prosecution of offenders.

2. In addition, information obtained from persons interdicted by U.S. law enforcement personnel may be retained in the Automated Biometric Identification System IDENT database for use by the Department of Homeland Security and other U.S. law enforcement agencies. Persons who believe information is inaccurately or improperly maintained in the IDENT database, may address requests for redress to: Program Management Office, U.S. Department of Homeland Security, Washington, DC 20528.