Privacy Impact Assessment
for the

U.S. Coast Guard

"Biometrics at Sea"

March 14, 2008

Contact Points
CDR Eric Riepe
USCG Office of Law Enforcement
(202)372-2166

Dr. Thomas Amerson
USCG Research and Development Center
(860)441-2894

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This Privacy Impact Assessment (PIA) describes expanding the existing U.S. Coast Guard (USCG) and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program partnership to provide mobile biometrics collection and analysis capability at sea, along with other remote areas where DHS operates. As a result of the success of this partnership's USCG Mona Pass Proof of Concept (POC), the USCG plans a measured expansion of at-sea biometric capability throughout its mission scope and areas of operation. This measured expansion of biometrics at sea will assist in the prosecution of persons engaged in such activities as illegal maritime migration, smuggling, illegal drug transportation, and other types illegal maritime activity. By deterring unsafe and illegal maritime migration and other illegal activities at sea, the use of biometrics will promote an important USCG mission, in particular the preservation of life at sea and the enforcement of U.S. law.

Introduction

The USCG Maritime Biometrics System PIA focuses on a measured expansion of the existing USCG use of technology and collection of biometric information from persons reasonably suspected of violations of U.S. law who are interdicted at sea or as a result of at-sea interdictions. This use of biometrics at sea builds upon a Proof of Concept (POC) conducted in the Mona Passage (Mona Pass) from November 2006 through the present. The Mona Pass POC refined the process of collecting biometrics in a maritime environment and enabled the USCG to evaluate many requirements for maritime ready, light weight, durable mobile biometrics collection equipment. USCG and US-VISIT will also incorporate the collected biometric information (digital fingerprints and 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. (For the purpose of simplification in this document, and in accordance with current DHS policy regarding the access of biometric databases, through IDENT, by DHS agencies, the term "DHS accessed databases" will be used as a collective term for these additional databases.) A phased approach for full implementation of biometric comparison capability is to be rolled out beginning with Coast Guard District Seven area of responsibility (AOR).

The USCG intends a phased deployment of at-sea biometric capability to reach four goals. First, provide the foundation to develop DHS mobile biometric capabilities. Second, provide 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, etc.), by providing additional identifying information of interdicted persons not available without at-sea biometrics collection and analysis. Third, deter human smuggling networks by improving enforcement of U.S. Immigration Laws, 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). 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. Experience demonstrates that as prosecutions increase fewer undocumented aliens attempt the dangerous and illegal passage to the U.S. via maritime means. Through the at-sea screening process, USCG will collect biometric information only from appropriate individuals who are the focus of law enforcement efforts including without limitation enforcement of 8 U.S.C. § 1324-1327. Anyone providing appropriate documentation to verify their status within the U.S. will not have biometric information collected unless there are reasonable grounds to suspect such documents may be fraudulent or

due to exigent circumstances 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 U.S. will be processed in accordance with pre-existing approved procedures for interdiction and entry into the United States.

Participating Coast Guard cutters are capable of transmitting biometric data (digital fingerprints and 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.).

As fully 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:

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,
3. Completes the Coast Guard cutter patrol (typically 3-5 days).

The USCG does not maintain its own biometric database.

The USCG intends to use maritime biometrics for law enforcement (LE) activities; primarily for Alien Migrant Interdiction Operations (AMIO), but may also use biometrics capabilities to support other LE/maritime homeland security (MHLS) operations.

The USCG's alien maritime interdiction operations (AMIO) are directed to the unsafe transportation of migrants by sea which 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). Illegal 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 LE, national, and HLS 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. The USCG maritime biometrics system merges portable biometrics technologies and capabilities available through US-VISIT and the IDENT database and enhances the USCG's ability to perform its missions.

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

The USCG is prepared to conduct a phased in deployment of maritime biometrics in support of its law enforcement and homeland security missions, with particular emphasis on AMIO in the Area of Operations of the Seventh Coast Guard District, but without limitation to that AOR. This PIA recognizes a general use of maritime biometrics by the USCG as it expands its biometrics program.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The USCG will collect biometric information conforming to US-VISIT protocol (currently either two digital fingerprints, one of each index finger or an alternate finger if the index finger is missing, or 10 flat fingerprints and a digital photograph) from persons who the USCG interdicts at-sea who are reasonably suspected of attempting to enter or re-enter the U.S. in violation of U.S. law or of other violations of federal law (such as maritime drug trafficking). The USCG will obtain biometric information from persons at the same time it obtains basic biographic information (e.g., name, gender, date of birth, nationality, departure point, date of departure, destination point, and ID of the master, if available) in connection with routine processing.

The USCG uses at-sea screening to ascertain claims of U.S. or other citizenship and/or immigration status in the United States. Persons presenting facially valid documents of status in the U.S. will be processed in accordance with pre-existing approved procedures for entry into the United States. U.S. citizens or persons with immigration status in the U.S. (e.g. parolees or legal permanent residents) who are reasonably suspected of violations of federal law (i.e. migrant smuggling in violation of 8 U.S.C. 1324) may have their biometrics taken after interdiction at sea in connection with investigation of such criminal activity. U.S. citizens or persons with immigration status in the U.S. (e.g. parolees or legal permanent residents) whose biometric information is inadvertently enrolled in IDENT may seek correction or redress, as appropriate, as described in paragraph 7.2.

1.2 What are the sources of the information in the system?

The USCG will obtain biometric data from persons reasonably suspected of violations of U.S. law who are interdicted at sea or as a result of at-sea interdictions. USCG personnel will obtain biometric data from such persons while performing duties within the scope of their authority under U.S. and international law. Anyone providing appropriate documentation to verify his or her status within the U.S. will not have biometric information collected unless there are reasonable grounds to suspect such documents may be fraudulent or due to exigent circumstances 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 from whom biometric data may be obtained may include, but are not limited to:

1. Undocumented aliens who are attempting to enter or re-enter the U.S. in violation of U.S. law;
2. Persons reasonably suspected of migrant smuggling in violation of U.S. law;
3. Other persons interdicted at sea in connection with AMIO;
4. Persons reasonably suspected of maritime drug trafficking;
5. Persons reasonably suspected of terrorist activity or support of terrorist activity in violation of U.S. or international law (including activity defined or described in 18 U.S.C. 2331-2332f, 2339, 2339A-C);
6. Confirmation of crew identity in security boardings[1] or other suspected violations of U.S. laws with respect to vessel master and crew nationality on U.S. flagged vessels;
7. Identification of persons in Search and Rescue operations;
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.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected for near real time screening and at-sea identification of persons encountered by the USCG. Information collected will be used to determine courses of action (prosecution, repatriation, or some other action). Referrals of persons to other U.S. authorities (i.e. Department of Justice) for prosecution will be in accordance with federal law in effect at the time and any applicable international law and agreements between the United States and other governments, to the extent applicable. Biometric information will be enrolled in the

[1] 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).

IDENT database for future identification of persons encountered by DHS. This information may be used to identify repeat offenders for prosecution or other action.

1.4 How is the information collected?

The information is collected through secure, portable biometric collection device (electronic and inkless) utilized during USCG processing of persons at-sea. Biometric data collection is by trained, uniformed USCG personnel in the performance of their official duties.

The data collected will be prepared for transmission on secure stand-alone non-networked laptops (the transfer of this data is currently via USB cable, encrypted flash drive, and potentially via a secure wireless transfer on the same vessel or to a nearby attending USCG vessel). All biometric information collected will be sent to US-VISIT directly via encrypted electronic means for comparison against the IDENT database and DHS accessed databases. All biometric information collected from persons encountered during identified USCG operations will be enrolled into IDENT in accordance with IDENT's System of Records Notice (SORN) and all associated laws. Transmission to IDENT is critical in order to compare biometric information obtained during USCG operations against all criminal populations in IDENT or DHS accessed databases. This will ensure that all relevant criminal history information is available to Coast Guard and DHS decision makers who will then be able to consider the information available from US-VISIT and other DHS applications to make decisions with respect to the disposition of encountered persons (i.e. repatriation, prosecution, etc.).

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

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). Legal authorities for the collection of information maintained in IDENT is set forth in the DHS System of Record Notice (SORN) applicable to the IDENT program (72 FR 31080, June 5, 2007). The USCG's use of IDENT data supports and is consistent with the SORN, with previous US-VISIT published PIAs relating to IDENT (including in particular the PIA for IDENT dated July 31, 2006).

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

In developing the USCG's mobile biometrics capability, USCG and US-VISIT identified the minimum amount of information necessary to be collected, reviewed, and maintained to support the USCG's law enforcement and homeland security missions. The information collected (digital

fingerprints and photograph) is minimally intrusive and collected while the person is on board a Coast Guard cutter deck during routine processing following an at-sea encounter. Moreover, USCG personnel only collect biometrics from persons who are reasonably suspected of criminal activity, non-compliance with U.S. law, or who are attempting unlawful entry into the U.S. at the border or the functional equivalent of the U.S. border. USCG interdicting units will ensure that accurate copies of identifying documents and information confirming alien status of persons on board (POB) (e.g. ID cards, passport, etc.) are obtained if available. Persons presenting facially valid documents of status in the U.S. will be processed in accordance with pre-existing approved procedures for entry into the United States.

Anyone providing appropriate documentation to verify their status within the U.S. will not have biometric information collected unless there are reasonable grounds to suspect such documents may be fraudulent or due to exigent circumstances 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. Biometric information collected will be compared against the entire IDENT database and DHS accessible databases to determine the identity of the person if known. This action gives the USCG, DHS and DOJ the ability to detain, arrest and refer persons for prosecution with greater certainty of the suspect's identity and current criminal and immigration history, if available.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The USCG will use collected biometrics information to determine if the persons interdicted at sea have an encounter history in IDENT or DHS accessible databases. 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 U.S.. 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 U.S.) and recidivist violators of U,S, immigration laws (i.e. persons with multiple prior removals from the U.S.). 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.

The USCG will also submit biometric and biographical information obtained from encountered persons for enrollment into IDENT. This information will be used by IDENT in the same way as all other encounter information. In turn, the collected information will enable the USCG to identify persons previously enrolled by the USCG in repeat encounters. The biometric

information will also be used to determine the continued efficacy of the USCG mobile maritime biometrics system and make improvements to the technology as needed.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

USCG personnel will capture biometric data (digital fingerprints and photographs) with devices capable of scanning accurate digital fingerprints and taking accurate digital photos. Biometric information is collected by trained USCG personnel 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, periodic reviews of IDENT quality scores for USCG enrollments will be made 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.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above-described uses.

Specific guidance on data control will be provided to participating USCG personnel in a localized Concept of Operations (CONOPS) to ensure consistency in data handling. The USCG will not retain any of the biometric data that it obtains from undocumented aliens or other persons encountered at sea. Once the data are submitted to US-VISIT and enrolled into IDENT, the biometric information initially collected at sea is purged from the USCG laptop and workstation. Any portable hand-held devices on which basic biometric information is collected shall be fully erased upon successful transfer of data to the secure stand-alone laptop.

USCG will only be able to enroll and search through a scripted biometrics exchange. USCG will not be able to enter and search biometric databases by biographic information. This minimizes the risk of inappropriate use of biometrics because the system can only be searched if a biometric is presented and uploaded into the system for matching.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

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

All data from the initial biometric collection at sea will be deleted and erased from all USCG systems upon confirmation of successful enrollment into the IDENT database and therefore not retained by the USCG. 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.

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

Yes, the retention schedule for IDENT data has been approved.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The biometric information collected by the USCG is retained on any stand alone or USCG systems only until the appropriate information is confirmed as successfully enrolled into the IDENT system. 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.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared?

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.

4.2 For each organization, what information is shared and for what purpose?

USCG allows sharing of the biometric data contained in the recidivist portion of IDENT, for the purposes consistent with the current uses of the recidivist portion of IDENT for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions and to provide associated testing, training, management reporting, planning and analysis, or other administrative uses that require the use of biometrics to identify or verify the identity of individuals. The USCG has consented to IDENT sharing information supplied for inclusion in the recidivist portion of IDENT with any appropriate party per these terms through a Biometrics 'Memorandum of Understanding' between US-VISIT and the USCG'.

USCG will share biometrics (digital fingerprints and digital photograph and biographic information (name, gender, date of birth, nationality, if available).

4.3 How is the information transmitted or disclosed?

The USCG data in IDENT will be transmitted between IDENT and other systems on the DHS core network, an unclassified, secured wide area network. The data collected by the USCG are transferred to the USCG network by an encrypted flash drive (from laptop to a USCG standard workstation). The data are transmitted from the USCG to IDENT, through an unclassified, link-encrypted secure satellite connection. If data must be air-gapped to a shoreside USCG workstation due to lack of satellite connectivity or failed signal, USCG personnel shall maintain positive control of the data (on flash drive, hard drive, etc.) until transmitted to IDENT or the applicable database. After transmission and receipt acknowledgement the data will be erased from the flash drive, hard drive, etc. that was used for transport.

4.4 Privacy Impact Analysis: Given internal information sharing, discuss what privacy risks were identified and how they were mitigated.

DHS internal data sharing is required to comply with statutory requirements for national security and law enforcement. In all cases however, this data must be kept secure, accurate, and appropriately controlled. The USCG and US-VISIT ensure that any privacy risks are mitigated through data sharing agreements that require such things as auditing, access controls, re-sharing limits, and other physical, technical, and administrative controls.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared?

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.

5.2 What information is shared and for what purpose?

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 with any appropriate party per these terms.

5.3 How is the information transmitted or disclosed?

The USCG data included IDENT data is typically transmitted or disclosed to external organizations in one of three ways:

• Direct limited access to IDENT where personnel of these organizations are co-located with DHS personnel with access to the system;

• Limited direct connections to other systems where data may be transmitted directly between IDENT and those other systems; and

• Data are securely transferred on portable media when there is no direct connection between systems.

In all instances the information will be transferred via secure or encrypted means.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom· information is shared, and does the agreement reflect the scope of the information currently shared?

DHS has entered into MOUs or other agreements with non-DHS organizations with which IDENT shares information. These agreements provide the conditions of sharing or disclosure, including governing the protection and use of the information. The USCG's use of IDENT data does not modify, affect or impact these DHS MOUs. The information collected by USCG will be maintained in the recidivist portion of IDENT and shared in the same manner that other data in the recidivist portion of IDENT is shared within DHS. Any sharing of the USCG data in the recidivist portion of IDENT with an external organization would be governed by an existing DHS MOU or similar agreement covering the use of this type of data with such organization and would not require a separate USCG MOU or agreement with such organization.

5.5 How is the shared information secured by the recipient?

External connections must be documented and approved with each party's signature in

an interagency security agreement (ISA) that outline controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which IDENT shares information must agree to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information. Furthermore, recipient organizations must notify DHS as soon as reasonably practicable, but no later than within 24 hour period, after they become aware of any breach of security of interconnected systems or unauthorized use or disclosure of personal information. The USCG's use of IDENT data does not alter these arrangements.

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

All IDENT information users must participate in a security and privacy training program either provided or approved by DHS. Consultants and contractors must also sign a non-disclosure agreement. All government employees and contractors are required to complete privacy training when they initially join the USCG. Subsequent yearly privacy refresher training is required of all government employees and contractors.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

To mitigate the risk of lost biometric data, the USCG data is safeguarded under the same privacy and security policies and procedures as other information in the recidivist portion of IDENT. Data shared with external organizations must be kept secure, accurate, and appropriately controlled. The USCG and US-VISIT ensure that any privacy risks are mitigated through data sharing agreements that require such things as auditing, access controls, re-sharing limits, and other physical, technical, and administrative controls.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the Individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If

notice was not provided, why not?

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.

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

The USCG use of IDENT data and collection of biometric information relates directly to DHS national security, law enforcement, immigration, intelligence, and DHS mission purposes. Therefore, there is no opportunity or right of undocumented aliens or suspected criminals interdicted by the USCG at sea to decline to provide the subject biometric and limited biographic information.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The DHS national security, law enforcement, immigration, and DHS mission related purposes for which the information is collected, allows no such right.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk identified was the potential loss of biometric data. In developing the USCG's mobile biometrics capability, USCG and US-VISIT identified the minimum amount of information necessary to be collected, reviewed, and maintained to support the USCG's law enforcement and homeland security missions. The information collected (digital fingerprint and digital photograph) is minimally intrusive and collected while the person is on board a Coast Guard cutter deck during routine processing following an at-sea encounter. Moreover, USCG personnel only collect biometrics from persons who are reasonably suspected of criminal activity, non-compliance with U.S. law, or who are attempting entry into the U.S. at the border or the functional equivalent of the U.S. border. USCG interdicting units will ensure that accurate copies of identifying documents and information confirming alien status of

persons on board (POB) (e.g. ID cards, passport, etc.) are obtained if available. Persons presenting facially valid documents of status in the U.S. will be processed in accordance with pre-existing approved procedures for entry into the United States. Mitigation of the privacy risks for the minimal biometric and biographic data collected consists of the physical and system security safeguards and in the individual's right of access, redress, and correction as described in Section 7.0.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

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. However, in cases in which access is not prohibited, individuals may request access to their data directly through the redress process or other means as provided for by US-VISIT.

7.2 What are the procedures for correcting erroneous information?

Individuals may have an opportunity to correct their data when it is being collected, otherwise, they may submit a redress request directly to the US-VISIT privacy officer who will work with USCG to properly respond. The US-VISIT website, www.dhs.gov/us-visit, provides procedures and a Redress Request Form for correcting information. If individuals do not have access to the US-VISIT web site, they may request a copy of the Redress Request Form and instructions directly from the US-VISIT Privacy Officer by calling 202-298-5200. Requests should be sent to US-VISIT Program, U.S. Department of Homeland Security, Washington, D.C. 20528, USA. If an individual is not satisfied with the response received from US-VISIT, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and provide final adjudication on the matter. Appeals should be sent to Chief Privacy Officer, U.S. Department of Homeland Security, Washington, D.C. 20528, USA. If an individual with status in the U.S. believes that his/her fingerprints have been inappropriately included in IDENT as part of the USCG

POC, the individual should provide a copy of appropriate documentation demonstrating status within the U.S. to the above address. If after appropriate review and determination that the individual has appropriate status within the U.S., the information will be deleted from the recidivist portion of IDENT or other applicable database.

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

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. Contact information for the US-VISIT Privacy Office is available on the Internet, at www.dhs.gov/us-visit. USCG facilities in Sectors may also refer individuals who have requests for redress to the US-VISIT Privacy Office or related office applicable to each utilized database.

7.4 If no redress is provided, are alternatives available?

In the case of redress requests for DHS organizations, if an individual is not satisfied with the response from US-VISIT, the individual can appeal his or her case to the DHS Chief Privacy Officer, who may conduct a review and provide final adjudication on the matter.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided and, if access, correction and redress rights are not provided please explain why not.

Given that biographic information is provided directly by the individual, the need for redress will be limited to cases in which persons provided untruthful information or the USCG collection of biometric information did not function as intended. In all cases, including cases in which persons provide untruthful information that they later wish to correct or in instances in which biographic information associated with obtained biometrics (fingerprints/photos) is not accurate, redress procedures established and operated by US-VISIT will adequately and appropriately deal with requests for redress under these and other circumstances. In the case of redress requests for all DHS organizations, if an individual is not satisfied with the response, an individual can appeal his or her case to the DHS Chief Privacy Officer who will conduct a review and provide final adjudication on the matter. In addition, persons from whom biometric

information was obtained may inform USCG personnel of any perceived errors at the time of collection and USCG personnel will take appropriate action at the time of collection to correct any actual errors.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

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.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes.

Contractors employed to develop and manage technology associated with the USCG collection of biometric data will have access to IDENT data. The extent of access will vary based on the need to fulfill the requirements of the contract under appropriate non-disclosure and use limitations.

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

Yes.

Access to IDENT is assigned based on the specific role of the users. Roles are created for each level of access required for individuals to perform their job functions. Examples of roles

include basic user, system administrator, system auditor, and system manager. With respect to the biometric information that the USCG obtains during interdictions, only authorized USCG personnel (including contractors) who require access to the equipment and data used by the USCG 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- VIST/IDENT in the performance of their duties.

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

DHS has documented standard operating procedures to determine which users may access IDENT. The minimum requirements for access to IDENT information are documented in security documentation, and include a DHS security clearance, security and privacy training, and need based on job responsibility. Access to information that is contained in the handheld and on the laptop is limited as per USCG Biometrics Standard Operating Procedures and is consistent with the USCG US- VISIT MOU for data sharing. Basic features include individual log on, user privileges and administrator privileges and physical security procedures. Any system that contains data will be stored in a secure location when not in use.

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

Access roles are assigned by a supervisor and are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access will be removed from the access list. Access is audited and the audit logs are reviewed on a regular basis.

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

USCG personnel will comply with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems. This handbook establishes a comprehensive program to provide complete information security including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. USCG personnel involved in the USCG collection of biometrics will receive training specific to all biometrics related security

requirements. All log information including audit logs is included in the USCG Biometrics Standard Operation Procedures. Audit logs are maintained for the download and upload of information between the biometrics collection device, non-networked stand-alone laptop, the flash drive, any transfer media, and the upload to the recidivist portion of IDENT.

All data stored on any media as part of USCG collection of biometrics is stored on encrypted media such as a hardware encrypted laptop or flash drive. Biometric data obtained on portable hand held devices is stored temporarily and erased upon transmission to the laptop. All data from the initial biometric collection at sea is erased from the laptop and flash drive at the end of the patrol and upon confirmation the information was successfully enrolled in IDENT. Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information.

IDENT is the only system of records to which the USCG will submit data obtained in connection with the USCG collection of biometrics. The USCG will not retain any of the biometric data initially collected at sea that it obtains from undocumented aliens or other persons encountered at-sea once the initial biometric data are submitted to US-VISIT and enrolled into IDENT. The data are purged upon confirmation of enrollment and are maintained only in the IDENT system. Portable hand held devices on which basic biometric information is collected shall be fully erased upon successful transfer of data to the stand-alone laptop. The laptop computers are stand-alone non-networked computers. The laptops will also be stored in approved security containers aboard the cutters or in secure command center spaces ashore when not in use. Only USCG personnel with a need to know and need to use the equipment and IDENT data in the performance of their duties will have access to the equipment and laptop. Data will be stored on portable encrypted media to further enhance information security. The USCG collected biometric data shall be deleted from the flash drive and laptop upon confirmation of the receipt of the biometric data to IDENT and enrollment into the IDENT database. The encrypted flash drives will be stored in approved security containers when not in use. The laptop computers will either be in an approved storage container within the designated Sector 24 hour watch center or on board the USCG vessel. The USCG patrol boats will typically be at sea for 3 to 7 days; Medium Endurance Cutters 30 to 60 days, and High Endurance and National Security Cutters vary by mission assignment.

lDENT secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application roles. IDENT is periodically evaluated to ensure that it complies with these security requirements.

IDENT has a robust set of access controls including role based access and interfaces which limit access to the appropriate discrete data collections to which users should have access. Misuse of

data in IDENT is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established roles of behavior, and be adequately trained regarding the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

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

All USCG personnel who receive access to lDENT or other data shall be appropriately educated and trained using USCG and DHS approved training modules addressing the proper treatment of personal information and proper care of the information systems to ensure the overall safeguarding of the information.

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

Yes, Interim Authority to Operate was completed on March 7, 2008

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The risks identified are the potential for unauthorized access to biometric data. To mitigate this risk, DHS has a robust security program that employs physical, technical and administrative controls. These controls are validated through a Certification and Accreditation process on a regular basis. Users have limited access that is established based on their role. Users are trained in the handling of personally identifiable information. The use of the laptop and handhelds will conform to the USCG Biometrics Standard Operating Procedures and the Memorandum of Understanding with US-VISIT. While at sea the Commanding Officer or the Executive Officer, in the absence of the Commanding Officer, of the USCG vessel will maintain authority and supervision over the handheld devices and laptops to ensure the integrity of the biometrics system. The laptops will be maintained in a secure portion of the vessel during use which will reduce the risk of loss or comprise of the laptop. The information will be stored on encrypted media throughout the process so that the information can not be retrieved if the laptop or portable media are compromised or lost.

The integrated communications solution enabling secure, encrypted communications with US-VISIT for the transmission of biometric data incorporates the following security features.

Information obtained on the portable encrypted handheld units is password protected. Once that information is transferred to the encrypted laptop on board USCG vessels it is secured as described above and data on the handheld units is erased automatically. Electronic biometric/biographic files are then transferred from the laptop to an AES256 encrypted thumb drive and subsequently transferred to Coast Guard standard workstations connected to the link encrypted Coast Guard Data Network Plus (CGDN+). The files are sent as attachments via electronic mail to US-VISIT for matching. The CGDN+ wide area network is certified and accredited for handling For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) data. The cutter's satellite connection is an extension of the CGDN+ and is also encrypted (cutter router to shore side router).

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

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

The USCG maritime biometrics system was built through a mixture of ground up and purchased and installed systems. It uses various existing hardware and software never before used together as one system. Off-the-shelf portable handheld devices for the collection of digital fingerprints and digital photographs were purchased, operating hardware and software were designed, developed and integrated by the USCG Research and Development Center based upon existing commercial technology and customized hardware and software that would meet the needs of the USCG.

The USCG maritime biometrics system does not change the IDENT biometrics collection and processing system.

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

The USCG adopted the DHS privacy risk management process based on information life cycle analysis and fair information principles in developing biometrics collection devices for use in collecting biometric information pursuant to the Biometrics Proof of Concept (PIAs dated Nov 3, 2006 and May 15, 2007) and continuing with the USCG collection of biometrics. Technical and programmatic design choices are informed by this approach, which analyzes proposed changes in terms of their life-cycle processes-collection, use and disclosure, processing, and retention and destruction-and the potential they may create for noncompliance with relevant statutes or

regulations (the Privacy Act in particular) or for violations of fair information principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

The following actions have been taken:

-Certification and Accreditation was conducted with the satellite communications data transfer mobile solution (phase two).

- The USCG maritime biometrics system will use secure, link encrypted communications to transfer collected data back to the IDENT database and DHS accessible databases for searching, thus eliminating the risk inherent in a deployed dataset (phase one) and maintaining best possible data currency by using the full IDENT database (phase two).

- Tight technical control of the use of the USCG maritime biometric system at sea is maintained through the use of technology including the following: data maintained on encrypted media or transmitted via encrypted means throughout the lifecycle of the data from initial collection to the enrollment in the recidivist portion of IDENT and disposal of the data from portable media and inability to search the database by anything other than a biometric,

- Tight physical security of the system, including the portable media and the laptops during operations, training and handling accountability for the system operators, physical isolation of the system while the vessel in underway, and system responsibility and accountability through the military chain of command.

9.3 What design choices were made to enhance privacy?

The USCG collection of biometrics employs several measures to enhance privacy. They are:

1. All portable storage devices are encrypted.
2. Technical access to equipment and data is strictly limited to a need-to-know/need-to-use basis for mission performance.
3. Physical access to the equipment is strictly limited to a need-to-use basis for mission performance
4. The laptop is maintained in a secure area of the vessel.
5. Equipment containing data is secured in approved security containers.
6. The USCG and US-VISIT incorporate strict security provisions, rules for access

and auditing requirements to ensure that information security is maintained.

9.4 Privacy Impact Analysis: Given the above choices regarding technology, what privacy impacts were considered and how were they resolved?

To minimize any privacy risks, all portable storage devices that contain biometric data are encrypted.

Access to equipment and data is strictly limited to a need-to-know/need-to-use basis for mission performance. Physical access to the equipment is strictly limited to a need-to-use basis for mission performance and the laptop is maintained in a secure area of the vessel. Equipment containing data is secured in approved security containers when not in use. The equipment developed and used in the proof of concept has undergone a Certification and Accreditation process. The MOU between the USCG and US-VISIT incorporates strict security provisions, rules for access and auditing requirements to ensure that information security is maintained.

Conclusion

The USCG and US-VISIT Program partnership and the USCG's capability will obtain four goals.

- Provide the foundation to develop mobile biometric capabilities for DHS.

- Provide decision makers with information to determine outcome of undocumented migrant interdiction, e.g. repatriate, deport, arrest, prosecute, etc., and of others encountered in interdictions such as counterdrug, terrorism, and security boardings.

- Provide a deterrent to human smuggling networks and attempts at illegal entry.

- Help preserve life at sea through deterrence.

The USCG uses at-sea screening to ascertain claims of U.S. citizenship and/or immigration status in the United States. Persons presenting facially valid documents of status in the U.S. will be processed in accordance with pre-existing approved procedures for entry into the United States.

This PIA outlines the measured expansion of the USCG maritime biometrics system, where the USCG has either integrated satellite communication solutions on board cutters or shoreside connections involved in biometrics collection. These communications allow all biometric information collected on undocumented aliens and others interdicted sent to US-VISIT via

encrypted electronic means for comparison against the entire IDENT database. After successfully testing the USCG's biometrics collection during a proof of concept period, the USCG maritime biometrics system will involve system integration for USCG and/or DHS mobile biometric applications. This PIA will be updated, as needed, to reflect appropriate system changes.

The USCG's access to IDENT is necessary because it contains data which can assist with USCG missions at sea while mitigating privacy risks through technology, process, and procedures. DHS has a rigorous security program employing physical, technical, and administrative controls to protect IDENT. DHS uses a privacy risk management process to ensure that all changes to IDENT do not significantly increase the risk to privacy.

To minimize any privacy risks associated with the USCG collection of biometrics, all portable storage devices, on which biometric data are stored, are encrypted. Access to equipment and data is strictly limited to a need-to-know/need-to-use basis for mission performance as stated in a USCG Biometric Standard Operating Procedures. Equipment containing data is secured in approved security containers. The equipment developed and used in the USCG Maritime Biometrics System has undergone a Certification and Accreditation process. The MOU between the USCG and US-VISIT incorporates strict security provisions, rules for access and auditing requirements to ensure that information security is maintained.

All biometric data collected at sea will be enrolled into IDENT to become a part of its permanent database. Upon successful receipt and enrollment of the data by US-VISIT the data are erased or destroyed by the USCG. The USCG will not permanently maintain any database with this biometric data.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security