Privacy Impact Assessment
for the

U.S. Coast Guard
"Biometrics at Sea"
Mona Passage Proof of Concept

November 3, 2006

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

CDR Gregory Buxa
USCG Office of Law Enforcement
(202) 372-2189

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(202) 227-3813

Abstract

This privacy impact assessment (PIA) describes the U.S. Coast Guard (USCG) and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program partnership. This project is in furtherance of the broader objective to develop mobile biometric capabilities for the Department of Homeland Security (DHS). The findings from this proof of concept will develop and refine technologies needed for mobile biometrics collection and analysis capability at sea, along with other remote areas where DHS operates. This deployment will assist in the apprehension and prosecution of illegal migrants and migrant smugglers. It will also deter unsafe and illegal maritime migration, which will help preserve life at sea. The USCG plans to deploy at-sea biometric capability during the operational Proof of Concept (POC) beginning in November 2006.

Introduction

The PIA focuses on the new collection of biometric information by the USCG using new technology at sea and incorporating the collected biometric information, plus limited biographical information, into IDENT. The Proof of Concept (POC) will be conducted from November 2006 through approximately April 2007. The Mona Passage (Mona Pass) POC will begin the process to understand the requirements necessary for maritime ready, light weight, durable biometrics collection equipment. This will provide the basis for full implementation of biometric comparison capability to be rolled out post-POC. The USCG will conduct the POC while doing its normal law enforcement missions in and about the Mona Pass.

The USCG intends to deploy at-sea biometric capability during the operational POC to reach four goals. First, the POC will provide the foundation to develop mobile biometric capabilities for DHS. Second, the POC will provide decision makers with information to determine outcome of undocumented aliens interdictions; e.g. repatriate, deport, arrest, prosecute, etc., by providing additional identifying information of interdicted undocumented aliens that is currently not available. Third, the POC will provide a deterrent to human smuggling networks by improving the enforcement of U.S. Immigration Laws, including 8 U.S.C. § 1334-1337. The POC will enable USCG and federal prosecutors to identify repeat offenders of immigration laws and other persons frequently interdicted in the Mona Pass. This will enable the USCG and federal prosecutors to better identify smugglers and persons involved in smuggling networks. Finally, it will help preserve life at sea because of the increased deterrence. As prosecutions increase in number and affect, undocumented aliens will be less likely to attempt the dangerous and illegal passage to the U.S. via maritime means and will have fewer opportunities to do so as smugglers and smuggling networks are effectively prosecuted. Through the at-sea screening process, USCG will ensure that biometric information will be

collected only from appropriate individuals that are the focus of law enforcements efforts, including enforcement of 8 U.S.C. § 1334-1337. 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.

Over forty (40%) percent of the undocumented aliens interdicted by the USCG since fiscal year 2004 tried to enter the United States illegally through the Mona Pass between the Dominican Republic and Puerto Rico. Among other factors, the lack of deterrence against migrant smugglers and difficulties with prosecution under current law contribute to the unabated flow of illegal migrants and migrant smugglers in this geographic area. In response to this threat, the USCG, in coordination with US-VISIT, Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and the Department of Justice (DOJ), developed and implemented national intra and interagency-cleared protocols to support migrant smuggling prosecutions in the Dominican geographic area under the auspices of the Maritime Operational Threat Response Plan. An essential element of these protocols is to identify at sea persons attempting to re-enter the United States illegally and other wanted felons through the matching of biometrics in the IDENT database and to prosecute these identified individuals.

Migrant interdiction occurs to control the "unsafe transportation of migrants by sea" as described and authorized in the Agreement between the Government of the United States of America and the Government of the Dominican Republic Concerning Cooperation in Maritime Migration Law Enforcement, signed by both countries on the 20th day of May 2003, (the US/DR bilateral agreement). The "unsafe transportation of migrants by sea" is defined in the US/DR bilateral agreement as all vessels not properly manned, equipped, or licensed for carrying passengers on international voyages, which would include all interdictions in this area. Most people interdicted at sea in the Mona Pass are not U.S. Citizens and are in violation of federal law. At a minimum such individuals are in violation of 8 U.S.C. § 1325 (attempted illegal entry into the United States). The illegal trade of human smuggling violates numerous federal laws and places the lives of migrants at grave risk. The ability to identify persons who have previously been deported, which is in violation of 8 U.S.C. § 1326; who have violated other immigration laws; who are wanted for other crimes; or who are persons on a terrorist watch list is critical to permit the USCG to fulfill its law enforcement and national and homeland security missions. This POC, which merges emerging portable biometric technologies with existing DHS biometric capability available through the IDENT system, will enhance the ability of the USCG to perform its missions.

In phase one of the POC, the USCG will augment the collection of biographic information of all undocumented aliens who the USCG interdicts in the Mona Pass with the use of portable hand-held devices with the capability to scan digital fingerprints and take digital photographs, while conducting Alien Migration Interdiction Operations (AMIO), according to

the Caribbean Border Interagency Group Migrant Smuggling Prosecution Standard Operating Procedures. The USCG will collect basic biometric information (two digital fingerprints, one of each index finger or an alternate finger if the index finger is missing, and digital photograph) at the same time the USCG obtains basic biographic information (name, gender, date of birth, nationality, and departure point, date of departure, destination point and ID of the master) from persons in connection with routine migrant processing on board a USCG vessel following interdiction and in accordance with the US/DR bilateral agreement and international law. Anyone providing documentation to verify their status within the US will not have biometric information collected.

USCG vessels on patrol in the Mona Pass area will have a stand-alone non-networked laptop computer on board that contains IDENT biometric records and associated fingerprint identification numbers (FIN) and the original source of the biometric data for a the portion of the IDENT database directly related to the interdiction mission. The IDENT data will be encrypted on the stand-alone non-networked laptops, which will be maintained in a secure area of the vessel during use and stored in approved security containers when not in use. The four database excerpts that the USCG will use come from the following IDENT data categories: 1) known and suspected terrorist, 2) aggravated felons, 3) previous deportees (deported felons and absconders) and 4) recidivists from Caribbean countries near the Mona Pass. The excerpted databases will be updated on a regular basis through encrypted exportable media downloads.

Upon completion of initial screening of undocumented aliens (in which initial safety and health screening processes occur), the USCG will upload the biometric data from the handheld to the stand-alone non-networked laptop computer to compare the biometric information collected on the handheld with the local database for any matches. The stand-alone laptop will be in a secure portion of the vessel during the processing. The results of this comparison will be a determining factor in how to process individuals interdicted at sea.

On a regular basis the USCG will upload for enrollment into the recidivist portion of IDENT, basic biographic information, associated fingerprints, and photos collected from undocumented aliens. This information will be wrapped into an encrypted Electronic Fingerprint Transmission (EFT) file prior to transmission to IDENT. In later phases of the proof of concept, the USCG will transmit encrypted EFT files directly to IDENT via secure communications lines (DHS intranet) for screening against the IDENT database in as close to real time as possible.

The USCG will retain no biometric data from the initial collection at sea after it has been submitted to and successfully enrolled in the IDENT database. The data collected at sea will be erased and/or destroyed after US-VISIT confirms that they have received and enrolled the data. IDENT will be the only database in which biometric data that the USCG obtains will be maintained.

Throughout the process all data will be encrypted, including portable media and the

stand-alone laptops. The stand-along laptops and the portable media will be secured in approved security containers when not in use.

During the second phase of the POC, the USCG will integrate communication solutions (satellite &/or cell-phone) on board the cutters being used in the POC. Because communications will be available, all biometric information collected on undocumented aliens will be sent to US-VISIT via encrypted electronic means for comparison against the entire IDENT database. Upon successful testing during POC phase one and two, the last phase of the POC should involve system integration for USCG and/or DHS mobile biometric applications. This PIA will be updated as the POC moves into phase two and three.

Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

The USCG will collect basic biometric information (two digital fingerprints, one of each index finger or an alternate finger if the index finger is missing, and digital photograph) from all persons who the USCG interdicts while conducting Alien Migration Interdiction Operations (AMIO). The USCG will obtain basic biometric information from interdicted persons at the same time it obtains basic biographic information (name, gender, date of birth, nationality, departure point, date of departure, destination point, and ID of the master, if available) from interdicted persons in connection with routine migrant processing following an interdiction. The fingerprints will be compared against the fingerprint template supplied from the IDENT. The IDENT data on the laptop includes the fingerprint templates, associated FIN numbers, and original source data for use in determining whether the individual should be prosecuted, deported, or repatriated.

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. U.S. citizens or persons with immigration status in the U.S. (e.g. parolees) whose biometric information is inadvertently enrolled in IDENT may seek correction or redress as described in paragraph 7.2.

1.2 From whom is information collected?

The USCG will obtain basic biometric data from interdicted migrants stopped as a result of the USCG migrant interdiction mission. The individuals include undocumented aliens, suspected smugglers, or other persons interdicted at sea in connection with AMIO.

1.3 Why is the information being collected?

The information is collected in order to screen and identify, at sea, and in near real-time, persons who are previous deportees or other immigration violators, felons, or persons on a terrorist watch list. The information collected will be used to determine whether the individuals will be prosecuted, repatriated, or be subject to some other action, including without limitation the prosecution of migrant smugglers or persons attempting to enter or re-enter the United States illegally, in accordance with various federal laws, including 8 U.S.C. § 1325 (attempted illegal entry into the United States), which is applicable to all migrant interdictions and consistent with the US/DR bilateral agreement. The information will also be enrolled in the IDENT database to identify repeat offenders for resulting prosecution or other action.

1.4 How is the information collected?

In the first phase of the POC, the information is collected through secure portable hand held devices capable of capturing digital fingerprints and digital photographs during processing of undocumented aliens following an interdiction event. The collection of this biometric data is conducted by trained, uniformed USCG personnel in the performance of their official duties.

The data collected on the hand-held device will be uploaded to secure stand-alone non-networked laptops via USB cable for comparison against the data contained in the local subset copy of the IDENT database, which will contain biometric and biographical information on known and suspected terrorist, aggravated felons, previous deportees (deported felons and absconders) and recidivists from Caribbean countries near the Mona Pass. During the first phase of the proof of concept this subset of the IDENT database will be updated approximately every two weeks.

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, 89; and 19 U.S.C. §§

482; 1401(i). 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 (71 Federal Register 42,651 (July 27, 2006)). 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 31 July 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 POC, USCG and USVISIT identified the minimum amount of information necessary to be collected, used, and maintained to support the mission of the program – a more efficient and effective means of identifying known and suspected terrorist, aggravated felons, previous deportees (deported felons and absconders) and recidivists from Caribbean countries near the Mona Pass. 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.

All undocumented migrant biometric information collected as part of the POC will be compared against the local IDENT database subset (known and suspected terrorist, aggravated felons, previous deportees (deported felons and absconders) and recidivists from Caribbean countries near the Mona Pass.) to determine the identity of the undocumented migrant, if known. The particular types of biometric information collected matches to the specific types of biometric information within the subset of the IDENT database being used for the purposes of this POC. This gives the USCG, DHS and DOJ the ability to detain arrest and prosecute illegal migrants and migrant smugglers.

Section 2.0 Uses of the system and 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 the information collected from all undocumented migrants to compare against the local IDENT database subset (known and suspected terrorist, aggravated felons, previous deportees (deported felons and absconders) and recidivists

from Caribbean countries near the Mona Pass) to determine the identity of the undocumented migrant, if known. This gives the USCG, DHS, and DOJ the ability to detain, arrest, and prosecute undocumented aliens attempting to enter the U.S. illegally and migrant smugglers.

IDENT data and the data that the USCG obtains from persons interdicted at sea during AMIO will be used by the USCG to identify and, if appropriate, prosecute undocumented aliens (or other persons) who are interdicted by the USCG at sea while attempting to enter or re-enter the United States illegally or who are suspected of other immigration or related offenses (e.g. migrant smuggling, failure to heave to, assault on law enforcement officers, assault on other persons such as migrants).

The USCG will also submit biometric and biographical information obtained from interdicted migrants for enrollment into the recidivist portion of 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 undocumented aliens in repeat encounters in migrant smuggling geographical areas. The biometric information will also be used to determine the efficacy of the new portable devices and make improvements to the technology.

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?

During the POC, USCG personnel will capture biometric data (digital fingerprints and photographs) with portable hand held devices capable of scanning accurate digital fingerprints and taking accurate digital photos. The portable devices incorporate quality check features that ensure the quality of fingerprints captured.

The interdicted migrants provide the limited biographic information about themselves in connection with the USCG's routine processing of undocumented aliens following an interdiction event. This may include statements or identifying documentation or both. Therefore, the biographic information is as accurate as the statements and documentation that the individuals provide.

During the first phase of the POC a subset of the IDENT database will used for

local searching. This database will be updated about every two weeks. This data will be as accurate and up to date as possible during the proof of concept. The USCG Cutter will typically be at sea for 5 to 7 days. If there is a match with the local database, the USCG will verify through IDENT that the data set against which biometric information was matched is current and accurate.

When downloading information from the mobile device 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 deleted from the local media until there is confirmation that the records have been 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.

IDENT is the only system of records to which the USCG will submit data obtained in connection with the Proof of Concept. The USCG will not retain any of the biometric data that it obtains initially from undocumented aliens or other persons interdicted at sea. Once the data are submitted to US-VISIT and enrolled into IDENT the biometric information initially collected at sea are purged and are maintained only in the IDENT system. The portable hand held devices on which basic biometric information is collected are equipped with "flash" memory which shall be fully erased upon successful transfer of data to the stand-alone laptop.

The IDENT subsystem on the stand-alone computers will be updated every two weeks. If there is a match, the USCG will contact US-VISIT to verify the status in the IDENT subsystem is still accurate. This will mitigate the risk of inappropriate action being taken because of non-current IDENT data.

USCG will only be able to match through biometrics. USCG will not be able to search the local subsystem by biographic information. This minimizes the risk of inappropriate use of the local subsystem 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 US-VISIT/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.

3.2 Has the retention schedule been approved by 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 information collected by the USCG is retained in the systems associated with the POC only until the appropriate information is uploaded into the IDENT system. After the information is uploaded to IDENT, the collected information is deleted from the stand-alone non-networked laptop computer. At this point, if the information is retained in any way on a POC system, it is only through its subsequent inclusion in the subset of IDENT data loaded to the standalone non-networked laptop computer.

Regarding the IDENT system, as an INS legacy system, the retention period for IDENT was established for holding the biometrics of subjects of interest in immigration and border management or law enforcement activities.

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 organizations is the information shared?

USCG will collect data on undocumented aliens and enroll them into the recidivist portion of IDENT. The USCG information obtained will only be uploaded into

the IDENT database and shared in accordance with policies that govern the use of recidivist data in IDENT. Specifically, this information may be shared with CBP, ICE, TSA, and USCIS.

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 Biometric Proof of Concept Standard Operating Procedure and a Memoranda of Agreement between US-VISIT and the USCG.

USCG will share biometrics (digital fingerprints and digital photograph and biographic information (name, gender, date of birth, nationality, departure point, date of departure, destination point, and ID of the master, if available).

4.3 How is the information transmitted or disclosed?

In most cases, 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 is transferred to the USCG network by an encrypted flash drive (from laptop to a USCG standard workstation). The data is transmitted from the USCG to IDENT, through an unclassified, secured network (DHS intranet). All data is encrypted prior to transmission to US-VISIT.

During the first phase of the proof of concept, IDENT data fingerprint templates, associated FINs and encounter types are sent approximately every two weeks on electronic media via approved sensitive but unclassified courier (e.g. FEDEX, DHL, etc.) to the USCG. This data is handled in accordance with the data classification of For Official Use Only (FOUO).

4.4 Privacy Impact Analysis: Given the internal 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 organizations is the information shared?

This POC will not directly share biometric information with any organization external to DHS. Any external sharing of the information collected will be through its inclusion into the recidivist portion of IDENT. As such, USCG will collect data on undocumented aliens and enroll them into the recidivist portion of IDENT. US-VISIT will then determine if it is appropriate to share with other external organizations. 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. The USCG information obtained will only be uploaded into the recidivist portion of IDENT and will not be shared by the USCG with any external organization.

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, departure point, date of departure, destination point, and ID of the master, 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 in 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 is securely transferred on portable media when there is no direct connection between systems.

In all instances the information will be encrypted.

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 pursuant to the Biometric Proof of Concept does not modify, affect or impact these DHS MOUs. The information collected by USCG will be uploaded into 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 in this POC 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.

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

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 Proof of Concept in Puerto Rico and in the Dominican Republic as well. 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?

Because the USCG use of IDENT data and collection of biometric information relates directly to DHS national security, law enforcement, immigration, intelligence, and related DHS-mission purposes, there is no opportunity or right of undocumented aliens interdicted by the USCG at sea to decline to provide the subject biometric and limited biographic information. For example, undocumented aliens interdicted in the Mona Pass showing intent to enter the U.S. are at a minimum in violation of 8 U.S.C. § 1325 or 1326 (attempted illegal entry/reentry).

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?

Because of the DHS national security, law enforcement, immigration, and DHS-mission related purposes for which the information is collected, no such right exists.

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

Only undocumented aliens or other persons who are interdicted at sea (aboard vessels that are typically not seaworthy) and who are attempting to illegally enter the United States are subject to the collection of the basic biometric information discussed in this PIA. Because interdiction takes place at sea and because the USCG's primary goal in all migrant interdiction cases is the safety of lives at sea, there is no opportunity for notice other than the publication of information discussed in Section 6.1 above. Moreover, because the USCG use of IDENT data and collection of biometric information relates directly to DHS national security, law enforcement, immigration, intelligence, and related DHS-mission purposes, there is no opportunity or right of undocumented aliens interdicted by the USCG at sea to decline to provide the subject biometric and limited

biographic information.

Section 7.0 Individual 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 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.

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 Sector San Juan Puerto Rico may also refer individuals who have requests for redress to the US-VISIT Privacy Office.

7.4 If no redress is provided, are alternatives are available?

In the case of redress requests for DHS organizations, if an individual is not satisfied with the response from US-VISIT, an 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 POC 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 Proof of Concept 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 in the Proof of Concept 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.

Contractors employed to develop technology associated with the Proof of Concept 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?

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 in the Proof of Concept 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 procedures 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 a USCG Biometric Proof of Concept Standard Operating Procedure 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. The laptop system will be locked up 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 (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 rules. USCG personnel involved in the POC will receive training specific to all POC security requirements. All log information including audit logs is included in the POC Mona Pass standard operation procedures. Audit logs are maintained for the download and upload of information between the mobile device, non-networked stand-alone laptop, the flash drive, and the upload to the recidivist portion of IDENT.

All data stored on any media as part of the POC is encrypted. The equipment that the USCG uses in the POC for obtaining biometric data uses the distributed data sets that US-VISIT will supply in the first phase of the program and all storage media on which biometric data is temporarily stored are secured in approved security containers when not in use. Biometric data obtained on portable hand held devices is stored temporarily on "flash" memory which is erased upon transmission to the laptop. All data from the initial biometric collection at sea is erased from the laptop upon conformation the information was successfully sent to 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 Proof of Concept. The USCG will not retain any of the biometric data initially collected at sea that it obtains from undocumented aliens or other persons interdicted at sea. Once the initial biometric data are submitted to US-VISIT and enrolled into IDENT the data are purged and are maintained only in the IDENT system. The portable hand held devices on which basic biometric information is collected are equipped with "flash" memory which shall be fully erased upon successful transfer of data to the stand-alone laptop. The laptop computers on which data sets from the IDENT database will be used in the first phase of the Proof of Concept are stand-alone non-networked computers. The laptops (no more than five are intended to be in use at any time during the Proof of Concept) will also be stored in approved security containers 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. Exportable media on which US-VISIT will distribute the local data sets from the IDENT database to the USCG in the first phase of the Proof of Concept will be stored in approved security containers when not in use. Data on portable media will be encrypted to further enhance information security. The USCG collected biometric data (EFT files) 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 Sector San Juan 24 hour watch center or on board the USCG Cutter. The USCG Cutter will typically be at

sea for 5 to 7 days.

IDENT 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 rules. 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 rules 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 IDENT data shall be appropriately educated and trained regarding 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?

The data currently residing in IDENT to be used in the USCG's Proof of Concept is secured in accordance with DHS and national-level security requirements, including the FISMA requirements. IDENT was granted an authority to operate in May 2005; this authority to operate will expire in May of 2008 unless reaccredidation is completed.

Equipment being developed and implemented as part of the USCG Proof of Concept is undergoing a Certification and Accreditation process to validate physical, technical and administrative controls. The final Certification and Accreditation package has been submitted. The Designated Approving Authority is expected to approve the Certification and Accreditation by 3 November 2006. USCG will encrypt all information

collected on the portable media. The stand-alone non-networked laptops will be maintained in a secure portion of the vessel during use. The US-VISIT data will be encrypted on the stand-alone non-networked laptops, which will maintained in a secure area of the vessel during use and stored in approved security containers when not in use. The stand-alone laptops and the portable media will be secured in approved security containers when not in use. All information will be transmitted in encrypted format to reduce the impact if the portable media are lost or otherwise compromised.

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

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 personal information. The use of the laptop and handhelds will conform to the Biometric Proof of Concept Standard Operating Procedure 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 Cutter 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 encrypted throughout the process so that the information can not be retrieved if the laptop or portable media are comprised or lost. The IDENT subsystem database is configured so that it can only be searched by biometric and not biographic information. This provides an additional layer of security in the event a compromise occurs with the laptop.

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 Biometrics at Sea POC was developed as an initial measure to test the

feasibility of biometrics collection at sea. It uses various existing hardware and software never used together as one system. Portable hand-held devices for the collection of digital fingerprints and digital photographs and operating hardware and software were designed, developed and put together by the USCG Research and Development Center based upon existing commercial technology and customized hardware that would meet the needs of the USCG.

The POC 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 hand-held biometrics collection devices for use in collecting biometric information pursuant to the Biometrics Proof of Concept. 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:

-Data shall be updated approximately every two weeks during POC. Even given the recidivism of the migrants attempting US entry from the sea, this frequency is considered sufficient.

-Only template data is provided rather than actual fingerprint images for the on-board mobile solution used in phase-one of the program. Sharing only template data is important because *if* the data is lost, no one would be able to use it to identify a person, whereas with fingerprint images, one could identify a person.

- Data encryption will be used to protect template data being shared with USCG.

-Certification and Accreditation is being conducted with both the on-board mobile solution (phase one).

- The proof of concept will use secure communications to transfer collected data back to the IDENT database for searching, thus reducing the risk inherent in a deployed dataset and maintaining best possible data currency.

- Tight technical control of the use of the USCG biometric system at sea is maintained through the use of technology including the following: data encryption 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 on the ship's bridge during operations, physical security of the data in approved storage containers when the system is not in use, 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 Proof of Concept employs several measures to enhance privacy. All data on portable storage devices is encrypted. Technical 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. The USCG and US-VISIT incorporates 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?

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

To minimize any privacy risks, all data on portable storage devices is 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. The equipment developed and used in the proof of concept is undergoing 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.

To minimize privacy risks from having inaccurate data on the IDENT subsystems, the USCG has put in place procedures for handling matches. In the event of a match, USCG will contact USVISIT before making a determination on an individual.

Conclusion

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

- It will provide the foundation to develop mobile biometric capabilities for DHS.
- It will provide decision makers with information to determine outcome of undocumented migrant interdictions, e.g. repatriate, deport, arrest, prosecute, etc.
- It will be provide a deterrent to human smuggling networks.
- And, it will help preserve life at sea.

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 first phase of the POC, where no direct communication solutions are available to the cutter. The lessons learned during the first phase will be built upon for later phases. During the second phase of the POC, the USCG will integrate communication solutions (satellite &/or cell-phone) on board the cutters being used in the POC. Because communications will be available, all biometric information collected on undocumented aliens will be sent to US-VISIT via encrypted electronic means for comparison against the entire IDENT database. Upon successful testing during POC phase one and two, the last phase of the POC should involve system integration for USCG and/or DHS mobile biometric applications. This PIA will be updated prior to phase-two or three.

The USCG's access to IDENT is necessary because it contains data, which can assist with USCG missions while at sea while mitigating the privacy risks through technology and process and procedures. DHS has created a rigorous security program

employing physical, technical, and administrative controls to protect IDENT, in a way that would be difficult and excessively costly to implement if this data were contained in separate systems, in different locations, but that all must still link together to provide DHS' required functionality. 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 Proof of Concept, all data on portable storage devices is 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 Biometric Proof of Concept Standard Operating Procedure. Equipment containing data is secured in approved security containers. The equipment developed and used in the proof of concept has undergone a Certification and Accreditation process. The data sets from the IDENT database that US-VISIT will distribute to the USCG via encrypted media for use on dedicated stand-alone laptops in the first phase of the Proof of Concept are also secured in approved security containers along with the laptops when not in use. The updated media will sent via approved sensitive but unclassified courier (currently FEDEX) on an as required basis to ensure currency of information. 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 initially collected at sea will be downloaded to IDENT to become a part of its permanent database and upon receipt and enrollment of the data by US-VISIT the data will be erased or destroyed by the USCG. The USCG will not permanently maintain any database with this biometric data.

Approval Signature

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security