Privacy Impact Assessment Update
for the

U.S. Coast Guard
"Biometrics at Sea" Program

May 15, 2007

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
(703) 235-0780

Abstract

This is an update to the previous Privacy Impact Assessment (PIA) for the U.S. Coast Guard (Coast Guard) Biometrics At Sea Mona Passage Proof of Concept, dated November 3, 2006. This update describes new means by which the Coast Guard will transmit information to the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Automated Biometric Identification System (IDENT) in connection with the Coast Guard Biometrics At Sea Mona Pass Proof of Concept program (the "Program"). With the addition of capabilities described in this update, the Coast Guard will be able to transmit biometric data obtained from undocumented aliens that the Coast Guard interdicts in the Mona Passage directly to US-VISIT via secure, encrypted satellite communications for analysis against the IDENT database. Biometric information to be searched against will no longer be stored on the laptops. If there is a communications failure, the Coast Guard may revert back to the ability to search biometric data against the distributed IDENT data sets on stand-alone non-networked secured laptop computers on board Coast Guard cutters more fully described in the November 3, 2006 PIA. This change in process will take approximately several working days to establish.

Introduction

The November 3, 2006 PIA and this Update focus on the Coast Guard's collection of biometric information, including two (2) fingerprints and digital photograph, using new technology at sea and incorporating the collected biometric information, plus limited biographic information, into IDENT. The Program began in November 2006 and will continue indefinitely. The Program currently focuses exclusively on operations in the Mona Passage (Mona Pass) and the surrounding Coast Guard Sector San Juan Area of Responsibility (AOR) as smuggling trends change because of this capability. The Program may also be potentially applicable and transportable to other vectors when specific threats exist, however the crews will be from Coast Guard Sector San Juan. As additional locations are added outside of the Sector San Juan AOR, Coast Guard will update this PIA with a list of other locations in the appendix. The Program will begin the process to develop and understand the requirements for maritime ready, light weight, durable biometrics collection equipment, business processes and information technology processes. This Program will provide the basis for full implementation of biometric comparison capability to be developed in other vectors and by other U.S. agencies.

The Coast Guard has deployed and will continue to deploy at-sea biometrics capability to achieve four goals. First, the Program will provide the foundation to develop mobile biometric capabilities for Department of Homeland Security (DHS). Second, the Program will provide Coast Guard, DHS and interagency decision makers with information to determine the outcome of undocumented alien interdiction (e.g. repatriation, deportation, arrest, prosecution, etc.) by providing additional identifying information about interdicted undocumented aliens that is currently not available without mobile

biometrics capabilities. Third, the Program will provide a deterrent to human smuggling networks by improving the 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 Program will enable Coast Guard and federal prosecutors to identify repeat offenders of immigration laws and other persons frequently interdicted in the Mona Pass and potentially other vectors. This will enable the Coast Guard and federal prosecutors to better identify smugglers and persons involved in smuggling networks. Finally, the Program will help preserve lives at sea because of increased deterrence to smugglers and violators of immigration laws. 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. The Coast Guard also uses at-sea screening to validate 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. Through the at-sea screening process, Coast Guard will ensure that biometric information will be collected only from appropriate individuals that are the focus of law enforcement efforts, including enforcement of 8 U.S.C. §§1324-1327.

Over forty percent (40%) of the undocumented aliens that the Coast Guard has interdicted each year since 2004 have attempted to enter the U.S. 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 heavy flow of illegal migrants and migrant smugglers in this vector. In response to this threat, the Coast Guard, 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 the prosecution of migrant smuggling and immigration offenses 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 those identified individuals.

Migrant interdiction attempts to halt the "unsafe transportation of migrants by sea" is defined 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 vector. For the most part, most persons interdicted at sea in the Mona Pass are not

U.S. citizens and are attempting to enter the U.S. illegally. At a minimum, such individuals are in violation of 8 U.S.C. §1325 (improper entry by alien). The illegal trade of human smuggling violates numerous federal laws and places the lives of migrants at grave risk. The ability to identify previously departed persons who are attempting to re-enter the U.S. (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 enabling the Coast Guard to fulfill its law enforcement and national and homeland security missions. This Program merges portable biometrics technologies and capabilities with DHS's existing biometrics capabilities available through US-VISIT and the IDENT database and enhances the ability of the Coast Guard to perform its missions.

Between November 17, 2006 (when the Program commenced operations) and April 14, 2007, the Coast Guard obtained biometrics from 596 undocumented migrants interdicted in the Mona Pass. Of those, 117 persons were identified in the IDENT database set distributed to Coast Guard cutters as described in the November 3, 2006 PIA. To date, persons interdicted in the Mona Pass and identified in the IDENT database have included convicted felons (including persons convicted of violent crimes, drug trafficking and gang related offenses), recidivist immigration violators and persons who have been subject to final orders of deportation. Based largely on the information made available through the analysis of biometrics in the Program, the U.S. Attorney's Office in San Juan commenced 26 new prosecutions for violations of U.S. immigration law through April 14, 2007.

Changes To The Program

Beginning on or about June 1, 2007, the Coast Guard will integrate communications equipment on board Coast Guard cutters capable of transmitting biometric data (fingerprint and digital photograph as described in the November 3, 2006 PIA) via efficient, secure, and encrypted means. This equipment will be installed on Coast Guard cutters already deployed with biometric equipment. With this updated and improved communications equipment installed on the Coast Guard cutters in this AOR (the area surrounding Coast Guard Sector San Juan as smuggling trends change because of this capability), Coast Guard cutters with deployed mobile biometrics equipment (the handheld units and other equipment described in the November 3, 2006 PIA) will be able to transmit all biometric information collected from undocumented aliens to US-VISIT directly via encrypted electronic means for comparison against the IDENT database. Electronic transmission to US-VISIT will occur immediately following the interdiction of the undocumented aliens and the capture of biometric information from each migrant on the portable hand-held equipment described in the November 3, 2006 PIA. Following successful transmission of all biometric data to US-VISIT, US-VISIT will compare the biometric information against the IDENT database and will communicate a "Hit" or "No Hit" response to any search results to the Coast Guard. Searching IDENT is critical in order to compare biometric information obtained from interdicted migrants against all criminal

populations in IDENT, as opposed to the smaller fraction of IDENT records used during initial evaluation of the Program. 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 interdicted undocumented aliens (i.e. repatriation, prosecution, etc.) in accordance with 8 U.S.C. §§1324-1327.

Existing biometrics capabilities available through the stand-alone non-networked laptop computers on which the distributed IDENT data sets described in the November 3, 2006 PIA and procedures for use of those capabilities and equipment will remain available for use on a temporary basis. The continued availability of the stand-alone non-networked laptop system described in the November 3, 2006 PIA is needed in the event of communications failures with the integrated communications solution described above.

As more fully described in the November 3, 2006 PIA, the Coast Guard will retain no biometric data from the initial collection at sea after it has been submitted to and successfully enrolled in the IDENT database. All such data will be deleted, erased and/or destroyed after the Coast Guard verifies that US-VISIT has received each data file and has enrolled the data, and after all of the subject undocumented migrants have been either repatriated or transferred to U.S. authorities ashore for prosecution, as material witnesses in a prosecution or for other processing in accordance with pre-existing approved immigration or other procedures and upon completion of the Coast Guard cutter patrol (typically 3-5 days). IDENT will remain the only database in which biometric data collected by Coast Guard is maintained.

Reason For Changes

This PIA update is provided based upon the pending implementation of the integrated communications solution on board Coast Guard cutters. This component of the Program was generally described in the November 3, 2006 PIA but is more fully described above.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There are no changes to the manner in which data is collected from interdicted migrants under the Program. Data collection remains fully described in sections 1.1 through 1.4 of the November 3, 2006 PIA. All biometric information collected from undocumented aliens will be sent to US-VISIT directly via encrypted electronic means for comparison against the IDENT database. All biometric information collected will be enrolled into IDENT. Searching IDENT is critical in order to compare biometric information obtained from interdicted migrants against all criminal populations in IDENT, as opposed to the smaller fraction of IDENT records used during initial evaluation of the

Program. 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 interdicted undocumented aliens (i.e. repatriation, prosecution, etc.) in accordance with 8 U.S.C. §§1324-1327.

Uses of the System and the Information

There are no new uses of the data being collected for the Program other than the transmission of data to US-VISIT via secure, encrypted communications for searching against the IDENT database described above. Other data use remains fully described in sections 2.1 through 2.4 of the November 3, 2006 PIA.

Retention

Information will continue to be retained in accordance with the IDENT schedule as noted in the November 3, 2006 PIA.

Internal Sharing and Disclosure

There are no additional data disclosures from Coast Guard. All disclosures and procedures for disclosure are fully addressed in sections 4.1 through 4.4 of the November 3, 2006 PIA.

External Sharing and Disclosure

There are no additional data disclosures from Coast Guard. All disclosures and procedures for disclosure are fully addressed in sections 5.1 through 5.7 of the November 3, 2006 PIA.

Notice

Notice is provided by this PIA update of Coast Guard's use of integrated communications solutions on board Coast Guard cutters to transmit biometrics data obtained from undocumented aliens to US-VISIT via secure, encrypted means. Notices described in sections 6.1 through 6.4 of the November 3, 2006 PIA remain in effect as well.

Individual Access, Redress, and Correction

As described in the November 3, 2006 PIA, the collected biometric data is used for law enforcement, immigration enforcement and national security purposes pursuant to Coast Guard authorities and there is no opportunity for persons to consent or to refuse to provide the data for the reasons fully described in the November 3, 2006 PIA. Procedures for redress are fully described in sections 7.1 through 7.5 of the November 3, 2006 PIA.

Technical Access and Security

Security measures are fully described in sections 8.1. through 9.4 of the November 3, 2006 PIA. In addition to the security measures described therein, 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 handheld units described here and in the November 3, 2006 PIA are password protected. Once that information is transferred to the proof of concept system on board Coast Guard cutters it is encrypted as described above and data on the handheld units is erased automatically. Electronic biometric/biographic files are encrypted at the file level, then transferred from the proof of concept systems to an AES-256 encrypted thumb drive and subsequently transferred to Coast Guard standard workstations connected to the Coast Guard Data Network Plus (CGDN+). The encrypted 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 shoreside router).

Technology

The Coast Guard has installed integrated communications equipment on board Coast Guard cutters capable of transmitting biometric data via efficient, secure, and encrypted means. Coast Guard cutters with deployed mobile biometrics equipment (the handheld units and other equipment described in the November 3, 2006 PIA) will be able to transmit all biometric information collected from undocumented aliens to US-VISIT directly via encrypted electronic means for comparison against the IDENT database. Electronic transmission to US-VISIT will occur immediately and the system described in section 9.2 of the November 3, 2006 PIA will not be used under normal situations. The satellite communication system on the cutters in the San Juan AOR is the Fleet 55 system, with service provided by INMARSAT spot beam coverage. This satellite connection is used to extend the Coast Guard Data Network Plus wide area network to the cutter's accredited local area network. As stated above, the satellite connection is encrypted from the cutter's router to the shoreside router.

Conclusion

The changes to the Program described in this Update will provide for a more efficient, comprehensive and convenient means of conducting the analysis of biometric data described in the November 3, 2006 PIA and this Update. This update will ensure that biometric data that the Coast Guard obtains from undocumented aliens is searched against the IDENT database ensuring that decisions with respect to disposition of the migrants are made based on the most current and most comprehensive information available. The update will also enhance the accuracy of identifying migrants as well as providing greater privacy and security protections by removing all biometric data from the laptops and onboard the cutters. The privacy risks of these revised procedures are minimal and have been mitigated through appropriate security procedures.

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security