Privacy Impact Assessment
for the

Biometric Exit Mobile Air Test (BE-Mobile)

DHS/CBP/PIA-026

June 18, 2015

Contact Point
Kim Mills
Entry Exit Transformation Office
U.S. Customs and Border Protection
(202) 344-3007

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) is conducting a Biometric Exit Mobile Air Test for certain aliens (which generally includes all non-U.S. citizens) departing the United States on selected international flights at selected U.S. airports. The Biometric Exit Mobile Air Test is designed to test a new biometric exit concept of operations at selected airports. During the test, CBP officers will use a wireless handheld device at the departure gate to collect biometric and biographic data and to test outbound enforcement policies and workforce distribution procedures. DHS is updating a previously issued Privacy Impact Assessment, entitled DHS/NPPD-001(j) Comprehensive Exit Program: Air Exit Program from 2009. The Department is also transferring the privacy compliance documentation for biometric air exit programs to the CBP privacy impact assessment inventory because CBP is the operational Component within the Department that is responsible for biometric and biographic entry and exit operations.

Overview

The Department of Homeland Security (DHS) established the United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) in accordance with statutory mandates[1] requiring DHS to create an integrated, automated, entry and exit system that records the arrival and departure of aliens, verifies aliens' identities, and authenticates aliens' travel documents through the comparison of biometric identifiers.[2] Per statute, certain aliens[3] may be required to provide biometrics (including digital fingerprint scans, photographs, facial and iris images, or other biometric identifiers) upon arrival in or departure from the United States.

On March 16, 2013, US-VISIT's entry and exit operations (including deployment of a biometric exit system) were transferred to U.S. Customs and Border Protection (CBP).[4] The Office of Biometric Identity Management (OBIM) within the National Protection and Programs Directorate (NPPD) was created to maintain the Automatic Biometric Identification System (IDENT), which is the Department's official biometric database. CBP assumed the biometric entry and exit operations on April 1, 2013.

---

[1] Immigration and Nationality Act (INA) §§ 215, 231, 262(a), 263(a), 264(c), 8 U.S.C. §§ 1185, 1231, 1302(a), 1303(a), 1304(c); Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. No. 104-208; the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Pub. L. No. 106-215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Pub. L. No. 106-396; the U.S.A. PATRIOT Act, Pub. L. No. 107-56; the Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Pub. L. No. 107-173; the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53.

[2] As used in this document, a "biometric identifier" is a physical characteristic or other physical attribute unique to an individual that can be collected, stored, and used to verify the identity of a person who presents himself or herself to a CBP officer at the border. To verify a person's identity, a similar physical characteristic or attribute is collected and is compared against the previously collected identifier.

[3] As used in this document, "certain aliens" are in-scope travelers subject to biometric air exit experiment consist of travelers who meet the criteria established under 8 CFR Part 215.8, which generally includes all non-U.S. citizens with certain narrow exceptions.

[4] See Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. 113-6, H.R. 933 (March 16, 2013).

CBP is developing ways to collect biometric information from certain departing aliens[5] (which generally include all non-U.S. citizens) in an effort to fulfill existing congressional mandates on biometric exit. As part of its ongoing efforts to implement a biometric exit program, CBP is conducting a Biometric Exit Mobile (BE-Mobile) Air Test that will be deployed to ten airports nationwide for one year. In this test, CBP officers use wireless handheld devices to collect biographic and biometric information from certain aliens upon departure in real time.

CBP will use the results of the test to help inform future plans for an air biometric exit system, which is a congressional mandate for CBP. One of the primary missions of the biometric exit program is to provide assurance of identity on departure of aliens within the scope of the pilot. This test will give CBP the opportunity to confirm aliens' identities, record their departure, run watchlist checks against aliens, and match departures with prior arrival records. CBP will use the results of the test to determine how to effectively implement an air biometric exit system.

Reason for the PIA Update

CBP is updating the existing DHS/NPPD/PIA-001(j) Comprehensive Exit Program: Air Exit Pilot that was first published on May 20, 2009.[6] The 2009 PIA described a test of a comprehensive exit program for integrating non-U.S. citizen departure with existing arrival information. The pilot program covered by the DHS/NPPD/PIA-001(j) concluded on July 2, 2009. Although the technology used in these pilot programs performed successfully, DHS concluded that the pilot's collection mechanisms would be extremely resource intensive and very costly to implement long-term or at additional airports, therefore, DHS did not expand or extend the 2009 pilot.

Scope of the Pilot

The BE-Mobile Air Test includes two biometric information collections. One biometric collection will rely on existing teams of CBP officers who conduct outbound enforcement operations to enforce U.S. statutes and regulations. CBP outbound enforcement operations include enforcing immigration statutes and trade or transportation outside of the United States (such as illegal narcotics, large amounts of cash, and other prohibited or regulated items). During the pilot, these existing outbound enforcement teams will record biometrics of the departure of certain aliens during standard outbound enforcement operations and on flights selected solely for the purposes of biometric exit recording.

The second biometric information collection will be randomly generated by statistical software. CBP will collect randomly selected biometrics of certain aliens before the departure of

[5] In-scope travelers subject to the biometric air exit experiment consist of travelers who meet the criteria established under 8 CFR Part 215.8, which generally includes all non-U.S. citizens with certain narrow exceptions.
[6] DHS/NPPD/PIA-001(j) – Comprehensive Exit Program: Air Exit Pilot PIA, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_air_exit.pdf.

one to five flights per week at each of the pre-selected airports. Statistical software is used to randomly select a certain number of flights from which to obtain biometrics. Flights can be randomized by time of day, carrier, and destination. The CBP Survey Team Supervisor will determine the most appropriate interval for processing certain aliens on a flight.

The BE-Mobile Air Test will be conducted at ten airports nationwide. The test will start at Hartfield-Jackson Atlanta International Airport no earlier than June 15, 2015, and will run for approximately one year. Over the course of the following five months CBP will deploy the BE-Mobile Air Test to nine additional airports, including:

- Los Angeles International Airport, Los Angeles, California;
- San Francisco International Airport, San Francisco, California;
- Miami International Airport, Miami, Florida;
- Chicago O'Hare International Airport, Chicago, Illinois;
- Newark Liberty International Airport, Newark, New Jersey;
- John F. Kennedy International Airport, Jamaica, New York;
- Dallas Fort Worth International Airport, Dallas, Texas;
- George Bush Intercontinental Airport, Houston, Texas; and
- Washington Dulles International Airport, Sterling, Virginia.

Technical Requirements

The BE-Mobile Air Test uses commercial off the shelf (COTS) hardware (Samsung S5s and Grabba fingerprint capture additions)[7] and a CBP developed software application to capture the biographic and biometric exit data from certain departing alien international travelers. CBP encrypts data on the wireless handheld device as it is collected. The biometric and biographic data are transmitted in a double encrypted secure HTTPS over a secure Virtual Private Network (VPN) tunnel to the Network Operations Center (NOC). CBP then transfers data in a double encrypted secure HTTPS over a secure VPN tunnel to the Targeting and Analysis Systems Program Directorate (TASPD) application server and then to both the Automated Biometric Identification System (IDENT)[8] and TECS.[9]

---

[7] Both the Samsung S5 and the Grabba fingerprint capture devices were vetted for security purposes and approved for use in the CBP environment.

[8] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system. IDENT is the central DHS-wide IT system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses. IDENT stores and processes biometric data (including digital fingerprints) photographs, iris scans, and facial images, and links biometrics with biographic information to

The BE Mobile Air Test requires collection of minimal biometric and biographic data from covered aliens to enable OBIM biometric matching, identity verification, and cross-checking against a list of subjects of interest on biometrics watchlists. This pilot is designed to test mobile technology whereby CBP officers using a wireless handheld device collect biometric and biographic data from certain aliens. The DHS/NPPD/PIA-001(j) PIA must be transferred to CBP and renamed and renumbered into CBP's inventory of PIAs as part of this update because US-VISIT's entry and exit responsibilities were transferred to CBP. Thus, CBP is now the operational Component within DHS that is conducting this information collection. .

Privacy Impact Analysis

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

Authorities and Other Requirements

The statutes that authorize DHS to create a biometric entry and exit have not changed since the DHS/NPPD/PIA-001(j) Comprehensive Exit Program: Air Exit Pilot that was first published on May 20, 2009.[10]

CBP's collection of biometric data for this project is covered by the DHS/CBP-007 Border Crossing Information (BCI) SORN.[11]

The BE-Mobile Air Test falls under the Automated Targeting System (ATS) authority to operate and system security plan. The BE Mobile Air Test falls within the ATS system security boundary to take advantage of ATS-Passenger interoperability with the biographic and biometric screening systems that CBP accesses for both entry and exit processing of travelers.

The information is covered by the Paperwork Reduction Act (PRA) and the OMB Number: 1600-0006.[12]

---

establish and verify identities. Handheld devices do not communicate with IDENT directly. Instead devices only transfer biographic and biometric information to the CBP Automated Targeting System (ATS) server, which then transfers the information to IDENT.

[9] DHS/CBP/PIA-009(a) – TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (August 5, 2011), *available at* http://www.dhs.gov/privacy-documents-us-customs-and-border-protection. TECS (not an acronym) provides computer-based access to enforcement files of common interest, on-line access to the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC), as well as an interface with the National Law Enforcement Telecommunications System (Nlets).

[10] DHS/NPPD/PIA-001(j) Comprehensive Exit Program: Air Exit Pilot PIA, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_air_exit.pdf.

[11] DHS/CBP-007 Border Crossing Information (BCI) SORN, *available at* https://www.federalregister.gov/articles/2015/05/11/2015-11288/privacy-act-of-1974-department-of-homeland-security-us-customs-and-border-protection-007-border

[12] http://www.gpo.gov/fdsys/pkg/FR-2010-03-09/html/2010-4905.htm

Characterization of the Information

For certain aliens (described under "Individuals Covered" below) selected for the BE Mobile Air Test, CBP will collect complete name; date of birth; gender; country of citizenship; passport number and country of issuance; country of residence; travel document type (e.g., visa), number, date, and country of issuance; departure information; and digital fingerprint scans.

Individuals Covered

For the duration of the BE Mobile Test, certain aliens must provide biometric information at the time of departure of the selected international flights at one of the selected airports, except for aliens exempt pursuant to 8 CFR 215.8(a)(2) provided that the alien is in exempted status on the date of departure. Exempted aliens include:

(1) Canadian citizens who under section 101(a)(15)(B) of the Immigration and Nationality Act are not otherwise required to present a visa or have been issued Form I-94 (see § 1.4) or Form 1-95 upon arrival at the United States;

(2) Aliens admitted on A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas who are maintaining such status at time of departure, unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to this notice;

(3) Children under the age of 14;

(4) Persons over the age of 79;

(5) Classes of aliens the Secretary of Homeland Security and the Secretary of State jointly determine shall be exempt; or

(6) An individual alien whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines shall be exempt.

Biometrics Collection Process

The BE-Mobile Air Test will be conducted on pre-selected outbound international flights either for outbound enforcement action or based on a statistical sampling that is necessary to inform CBP's future biometric exit planning. Statistical software is used to randomly select flights for each survey team. The variables may be weighted differently throughout the test to ensure the final survey population is proportional to typical airport operations and provides the most appropriate interval for processing certain aliens on a flight.

By estimating the participation of certain aliens on a flight, CBP can anticipate which processing interval may yield the number of certain aliens that will undergo processing in the

flight. For instance, if 75 percent of the flight is comprised of certain covered aliens and the team processes every second covered alien then the team will collect biometric information from nearly 38 percent of the flight. On a 200 passenger flight, this would result in collecting biometrics from approximately 75 travelers. The supervisor will determine which processing interval is operationally feasible taking into account the space of the boarding area in order to minimize disruptions to the flight boarding process.

For the selected flight, CBP officers deploy to the departure gate and position themselves near the departing passenger loading bridge to collect certain data from the departing alien passengers. Once passengers begin the departure process, CBP officers obtain biographic data from certain alien travelers by swiping or inputting the information from the alien's travel document (passport, visa, lawful permanent resident card, or other qualifying travel document) on a wireless handheld device.[13] CBP officers manually input the document's biographic details into the BE-Mobile device if the passport's information is not machine-readable.. Air carriers will continue to report departing passenger's travel document information to CBP as they do today.

CBP officers confirm whether the traveler is in-scope for biometric capture based on the travel document presented and the results displayed on the BE-Mobile device. If the traveler is in-scope, the BE-Mobile device prompts the CBP officer to capture the traveler's fingerprints. If the traveler is out-of-scope he or she may proceed to board the aircraft.

The biometric and biographic data collected during this experiment allows CBP officers to directly collect a passenger's travel document data and confirm the passenger's departure from the United States. Biometric data and limited biographic data will be stored in the DHS biometric database, IDENT. Biographic data will also be entered into the CBP law enforcement data system, TECS. Through these systems, CBP will record the departure of certain aliens, verify their identity, and screen each individual against biometric watchlists.

Enforcement Examinations

The CBP officer may decide, based on database search results as well as other factors such as the officer interview, that additional questioning and inspection are necessary. The interviewing CBP officer or a different CBP officer will conduct the additional inspection. If CBP determines that additional action is needed based on the biometric and biographic data collected from the individual, CBP will take appropriate action under its law enforcement authorities. The BE-Mobile Air Test will provide statistically valid observations of biometric exit in the commercial air environment for comparison to the baseline biographic exit system.

The biometric and biographic data will be used to confirm the individual's identity, check that individual against law enforcement databases to determine if that person is a wanted

[13] DHS/CBP/PIA-001(g) Advance Passenger Information System (APIS) (June 5, 2015), *available at* http://www.dhs.gov/privacy-documents-us-customs-and-border-protection. Air carriers will continue to report traveler information through the Advance Passenger Information System (APIS).

criminal or presents a national security or public safety risk, and record the individual's departure from the United States.

For out-of-scope aliens, the CBP officers record the departure of the alien to indicate that the alien has exited the United States. For certain aliens, the CBP officer will capture two fingerprints on the wireless handheld device from the alien's index fingers. CBP officers review the IDENT response and the alien is permitted to board the aircraft if there are no biometric watchlist hits. If there is a biometric hit the alien may be referred for further processing. If a certain alien refuses to provide his or her fingerprints, the CBP officer may refer the alien for further processing.

CBP performs multiple quality checks on biometric and biographic information to ensure the information is as accurate as current capabilities permit. Quality checks are conducted against the submitted documentation by verifying the information provided against a passport or another corroborating document (and if deemed necessary) by an in-person interview. Accuracy is also enhanced by providing individuals the opportunity to amend information if it is determined to be erroneous. Finally, robust multi-lateral administrative policies ensure inaccurate information is detected and corrected in a timely manner.

Privacy Risk: There is a risk that information could be inadvertently overheard by other travelers during an enforcement interview with a person that takes place during the boarding process.

Mitigation: CBP trains its officers to be aware of their surroundings to limit the likelihood that any sensitive information will be overheard by other travelers. The mobile devices being used for both biographic and biometric collection are designed to read the information from a travel document and fingerprint, so as to limit the amount of information shared in a more easily eavesdropped manner.

Uses of the Information

CBP uses the results of the test to help inform future plans for an air biometric exit system, which is a congressional mandate for CBP. One of the primary missions of the biometric exit program is to provide assurance of identity on departure of aliens within the scope of the pilot. This test will give CBP the opportunity to confirm aliens' identities, record their departure, run watchlist checks against aliens, and match departures with prior arrival records. CBP will use the results of the test to determine how to effectively implement an air biometric exit system. CBP will also use the results of the BE-Mobile Air Test to perform a statistical survey of the air outbound population to determine strategic programmatic requirements for a comprehensive biometric exit solution. The primary mission of any biometric exit program is to provide assurance of traveler identity on departure, giving CBP the opportunity to match the departure with a prior arrival record. This enhances the integrity of the immigration system and the ability

to accurately detect travelers who have overstayed the lawful period of admission to the United States. Additionally, CBP will use the results to perform a statistical survey of the air outbound population to identify the costs and benefits of such a biometric exit system, and to determine comprehensive biometric exit solutions.

CBP will analyze and evaluate the field test's success based on a number of criteria, including:

- The occurrence of watchlist matches based on biometric data;
- The occurrence of biometric-identified fraud;
- The occurrence of passengers not found on the APIS manifest;
- How overstay calculations are impacted;
- The transaction times for exit processing per passenger;
- The rate of successful transactions;
- The occurrence of law enforcement hits (including those requiring referral to secondary inspection);
- The observations from the CBP officers performing the test; and
- System performance.

Finally, the biometric data collected by the BE-Mobile Air Test and then stored in IDENT will be used to support immigration enforcement, management of immigration benefits, law enforcement, and other homeland security missions, as articulated in the IDENT SORN, the BCI SORN, and PIAs.

Privacy Risk: There is a risk that the biometric data may be inadvertently retained on the handheld mobile device.

Mitigation: The BE-Mobile Air Test process does not leave any data on the handheld mobile device. The handheld device is only used as a collection device, not a storage device. The biometric data is stored in IDENT. The software on the handheld device immediately transmits the collected biographic and biometric data to ATS-Passenger for processing and retention in a manner consistent with CBP's examination process at primary.

Privacy Risk: There is a risk that the biometric data may be inappropriately accessed during transmission to IDENT from the mobile devices.

Mitigation: All data remains encrypted during the entire transmission process. Fingerprints are not stored on either the Samsung S5s mobile device or the Grabba fingerprint capture device and are deleted upon transfer to the NOC. Devices remain in the control of a CBP officer at all times of use to minimize the potential for theft or loss. Mobile devices are stored at a secure CBP office at the airport when not in use. Mobile devices incorporate strict physical and

procedural controls, FIPS compliant data encryption, residual information removal, and require authorized users to sign in using account names and passwords to minimize privacy concerns.

Notice

CBP will provide tear sheets for passengers and fact sheets for other stakeholders. Please see a tear sheet example in Appendix B. Inasmuch as this will primarily be an enforcement effort, signage would be inappropriate under these circumstances.

To provide further notice to the public, CBP is publishing a new Federal Register Notice concurrent with this PIA update.

Privacy Risk: There is a risk that an individual may not be aware that CBP has launched a new biometric exit program that may collect their biometrics during some outbound travel but not others.

Mitigation: CBP provides notice of the collection and uses of information via publication of this PIA and Federal Register Notice. In addition, CBP is providing tear sheets to the persons who are subject to the biometric collection to inform them directly of the collection, CBP's authority, purpose, and use for the information. At the end of the test, CBP will review the tear sheets for adequacy, and any received comments concerning the effectiveness of the tear sheet, in conjunction with its review of comments received pursuant to the Federal Register Notice.

Data Retention by the project

The newly updated BCI SORN[14] states that for non-immigrant aliens, the information will be maintained for 75 years from the date of admission or parole into or departure from the United States in order to ensure that the information related to a particular border crossing is available for providing any applicable benefits related to immigration or for other law enforcement purposes. Air exit information is retained by the DHS biometric database IDENT in accordance with the approved IDENT retention schedule of 75 years. Please see the IDENT SORN and the IDENT PIA[15] for a full discussion of how this data is used and shared. Data stored on the mobile device will not be available on the device after it is transferred to IDENT and the data is immediately deleted from the device upon confirmation of its successful transfer to the IDENT system.

Privacy Risk: There is a risk that data will be retained longer than necessary to have mission value.

[14] DHS/CBP-007 Border Crossing Information (BCI) SORN, 80 Fed. Reg. 26941 (May 11, 2015).
[15] For more information please see the DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA, *available at* http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system

Mitigation: The record retention period of 75 years is consistent with the record retention period of BCI and the storage system for IDENT. This retention period reflects the need to maintain relevant biographic and biometric information pertaining to foreign nationals to support their possible intent to enter into the naturalization process for becoming a U.S. citizen. That process requires a comprehensive review of the applicant's travel history to the U.S. and his or her compliance with the statutory obligations for admission.

Information Sharing

There is no change with this update in the internal or external sharing and disclosure. Please refer to the IDENT PIA and supporting SORNs on how data (including data from the BE-Mobile Air Test) is shared with other government agencies.

All information sharing agreements must be reviewed and approved through an internal CBP process that includes a review by CBP policy and privacy officials, and the CBP Office of Chief Counsel. After CBP approves an information sharing agreement it is forwarded to DHS for final review and approval by all DHS Components.

Privacy Risk: There is a risk that prospective users who have not yet been approved as IDENT users will gain access to IDENT data through third party sharing.

Mitigation: The potential for unauthorized sharing is mitigated by implementing access controls to ensure that only authorized IDENT users can access the data, by placing limitations on third-party sharing, by limiting the amount of data shared based on specific circumstances described in information sharing access agreements, and by conducting periodic reviews of the use of the data with end users. The applicable data-sharing agreements require proper new user and use authorization. Lastly, all external sharing requires that the user responsible for sharing also account for that disclosure both to ensure consistency with the purpose and use provisions of IDENT and the Component system, and to permit auditing of the use of the data.

Redress

There are no changes with this update in the access, redress, and correction.

Privacy Risk: There is a risk that individuals, particularly non-U.S. persons, may not understand how to correct inaccurate information about themselves collected by CBP and stored in IDENT.

Mitigation: DHS TRIP provides a redress process through a website that facilitates the submission and processing of redress requests. Any individual can request access to or correction of his or her PII regardless of his or her nationality or country of residence. This process has

been described in the DHS TRIP PIA[16] and information is available in multiple places on DHS's public website. Additionally, the tear sheet contains contact information for DHS TRIP and the CBP Call Center for obtaining answers to questions.

Auditing and Accountability

The Office of Field Operations, Entry Exit Transformation Office uses strong documented standard operating procedures to determine which users may access information. Users accessing systems containing Air Exit information are required to hold appropriate security clearances and must complete mandatory security and privacy training annually. Furthermore, users are required to have a need to know the information based on their job responsibilities. Also, data is filtered based on the user, so that one user that has access to IDENT may have access to more or less data than another user. The Data Provider decides who may have access to the data it provides. Accurate event logs fully record all system access and the Information System Security Manager (ISSM) confirms compliance with the policy, and manages the activation or deactivation of accounts and privileges as required or when expired. Access control procedures operate in conjunction with a robust security program that implements physical, administrative, and technical controls to protect the confidentiality, integrity, and availability of the system.

In accordance with the access policies and procedures established by DHS and for DHS-owned systems, some contractors may have access to the systems that support Air Exit, in performance of their official duties (such as system administration, monitoring, and security functions). Contractor access is granted in accordance with the principles of least privilege, separation of duties, and need to know. The access policies and logs are reviewed by security management to ensure the effective implementation of privacy and security safeguards. Contractors are also required to possess appropriate security clearances and complete mandatory security and privacy training.

Privacy Risk: There is a risk that unauthorized users may access CBP biometrics stored in IDENT.

Mitigation: CBP has documented standard operating procedures to determine which users may access CBP data within IDENT. IDENT provides audit trail capabilities to monitor, log, and analyze system transactions, as well as actions and system accesses of unauthorized IDENT users. IDENT has a robust system of access controls, including role-based access and interfaces, which limit individual access to the appropriate discrete data collections. Misuse of the data in IDENT is mitigated by requiring that IDENT users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding

[16] DHS/ALL/PIA-002(a) - DHS Traveler Redress Inquiry Program (TRIP) (June 5, 2013), *available at* http://www.dhs.gov/privacy-documents-department-wide-programs.

the security of their systems. Also, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

Responsible Officials

Kim Mills
Entry Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-3007

John Connors
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
(202) 324-1610

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Biometric Entry/Exit Regulatory History

- January 2004 Interim Final Rule (69 FR 468) on Non-Immigrant Visa Travelers
  - Exit pilots were established in this rule, and updated later in 2004 in 69 FR 46556 and 69 FR 51695.
- August 2004 Interim Final Rule (69 FR 53318) on VWP Travelers and 50 Largest Land Ports
  - 50 Largest Land POEs identified in November 2004 (69 FR 64964)
  - Remaining Land POEs identified in September 2005 (70 FR 54398)
- August 2005 Notice With Request For Comments (70 FR 44934) on RFID Testing at Land Ports
- July 2006 NPRM (71 FR 42605) on Additional Alien Categories
- February 2008 NPRM (73 FR 8230) on Biometric Land Exit Test for H-2A Visa Holders
- April 2008 NPRM (73 FR 22065) on Biometric Air Exit
- December 2008 Final Rule (73 FR 77473) on Additional Alien Categories
- June 2009 Notice (74 FR 26721) on Biometric Air Exit Pilot at Two Airports

APPENDIX B

Tear Sheet Language for BE-Mobile

You have been selected to participate in a test to collect biometric data on handheld mobile devices.

Beginning in June 2015, U.S. Customs and Border Protection (CBP) will begin testing an enhanced handheld mobile device to collect biometric exit data from a limited number of foreign national travelers departing the United States to compare to the biometrics collected when the travelers entered the United States. CBP will analyze the information collected and use the results to inform future plans on biometric exit.

Q: Who is required to participate in the experiment? Is it mandatory?

A: Foreign national travelers who currently provide biometric (fingerprint) data as part of the arrival inspection process into the United States are required to provide biometrics upon departure if selected by CBP to participate.

Q: What information is captured during the exit inspection process?

A: A CBP Officer will collect the traveler's biographic information – data in the passport – and capture two index fingerprints.

Q: Will my personal data be shared or stored? How is my privacy protected if I give my biographic and biometric information?

A: Traveler data will be matched and stored in secure data systems managed by CBP and the Department of Homeland Security. CBP is dedicated to protecting the privacy of all travelers.

Q: How long will the experiment take place?

A: The experiment will run from June 2015 to June 2016, at select airports throughout the U.S.

Q: Where can I receive more information about this experiment and other CBP programs?

A: Please go to www.CBP.gov, or call the CBP Call Center at 202-344-1790.

Q: How do I obtain Redress?

A: DHS TRIP is a comprehensive traveler redress process to resolve inaccuracies and misidentifications. DHS TRIP may be contacted at: http://www.dhs.gov/step-2-how-use-dhs-trip. This website allows any individual the ability to request access to or correction of his or her personally identifiable information regardless of his or her nationality or country of residence.