Privacy Impact Assessment Update
for the

Conversion to 10-Fingerprint Collection for the

United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT)

November 15, 2007

Contact Point
Barbara M. Harrison, Acting Privacy Officer
US-VISIT Program
(202) 298-5200

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

Abstract

US-VISIT is an office and program within the National Protection and Programs Directorate of the Department of Homeland Security. The office manages DHS' IDENT system and provides biometrics-based identity management services to agencies throughout immigration and border management, law enforcement, and intelligence communities. The Program provides an integrated, automated, biometric entry and exit system that records the arrival and departure of foreign nationals. US-VISIT is publishing this Privacy Impact Assessment (PIA) to update and describe the US-VISIT Program's change from collecting two (2) fingerprints to collecting up to ten (10) fingerprints (using inkless optical reading devices) from foreign nationals upon entering or exiting the United States.[1]

Overview

The US-VISIT Program began its phased roll-out in January 2004. Each phase expanded the Program's capabilities, covered populations, or locations. Currently, US-VISIT collects 2 fingerprints, generally the right and left index fingers, from foreign nationals to associate an identity with biometrics collected from a first-time encounter or to verify the identity of an individual previously encountered, and to conduct various immigration, terrorism, and criminal background checks. The collection of only 2 fingerprints, however, limits US-VISIT's ability to more effectively match the prints in other governmental biometric databases. In particular, the Federal Bureau of Investigation's (FBI) Automated Fingerprint Identification System (IAFIS) is based on the collection of 10 fingerprints. US-VISIT's ability to submit 10 fingerprints against such databases will improve the likelihood of identifying known or potential criminals and terrorists. Moreover, the National Institute of Standards and Technology (NIST) advocates collecting more fingerprints to improve the accuracy of identifying individuals.[2]

US-VISIT will begin to collect up to 10 fingerprints at a limited number of ports of entry (POE) in late November 2007. Deployment to additional POEs is planned to begin in 2008. Since 2 fingerprints are already taken from foreign nationals arriving to the U.S., the only noticeable difference to a foreign traveler will be the collection of a greater number of (up to 10)

---

[1] This PIA updates the previously published *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)* (July 31, 2006); and *Privacy Impact Assessment for the US-VISIT Program In Conjunction with the Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Ports of Entry* (July 1, 2005).

[2] *See* Testimony of Dr. Martin Herman, Chief, Information Access Division, Information Technology Laboratory, National Institute of Standards and Technology before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, *Ensuring the Security of America's Borders through the Use of Biometric Passports and other Identity Documents* (June 22, 2005). http://www.nist.gov/testimony/2005/mherman_house_hs_biometrics_6-22.html.

fingerprints. US-VISIT will be testing two methods of collecting 10-fingerprints in order to determine the most effective and efficient method. In all cases, fingerprints will continue to be collected using inkless, optical collection devices. Methods to be tested will include: (a) the "three-slap process" where individuals provide four flat fingerprints from the right hand, four flat fingerprints from the left hand, and then simultaneous capture of the two thumbs; and (b) the "four-slap process," which requires four flat fingerprints from the right hand, and the right thumbprint, then four flat fingerprints from the left hand, and the left thumbprint. Once an individual's 10 fingerprints are collected and stored in DHS' Automated Biometric Identification System (IDENT), subsequent encounters, in most cases, will require the collection of fewer than 10 fingerprints for purposes of verification.

Section 1.0 Characterization of the Information

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

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

US-VISIT will continue to collect biometrics and limited biographic information as described in previous PIAs (available at www.dhs.gov/privacy, follow link to "Privacy Impact Assessments"). Instead of collecting 2 fingerprints as US-VISIT has done in the past, US-VISIT will now collect up to 10 fingerprints on first encounters with individuals. In subsequent encounters, some number of fingerprints less than 10 may be collected to verify the identity of a previously encountered individual.

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

Fingerprints are collected directly from the individual. Up to 10 fingerprints will be collected during an individual's encounter with a Customs and Border Protection (CBP) officer at a POE while going through the US-VISIT matching and verification process.

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

There is no change in the reasons why US-VISIT is collecting biometrics and biographics from foreign nationals, as described in previous PIAs. US-VISIT currently collects fingerprints from foreign nationals for purposes of allowing DHS to gauge admissibility by conducting various checks against immigration, criminal, and terrorism databases and lists. The transition from 2 to

10 fingerprint collection will improve US-VISIT's ability to effectively interoperate with other databases throughout the government, such as the FBI's IAFIS database. US-VISIT's ability to query 10 fingerprints against such databases will improve the likelihood of identifying known or potential criminals and terrorists simply because there is a higher accuracy and a higher match rate when the agency uses more fingerprints of an individual. Improving the likelihood of matching fingerprints will better support decision-making, potentially improving processing capabilities and enhancing privacy by more accurately identifying suspect individuals.

1.4 How is the information collected?

All foreign nationals subject to US-VISIT requirements will be required to provide up to 10 fingerprints, along with the same limited biographic information they provide currently, when processed through a CBP lane equipped with a 10-fingerprint scanner, in most cases on a first encounter. In all cases, fingerprints will continue to be collected using inkless, optical collection devices. There will be two collection methods tested: (a) the "three-slap process" where individuals provide four flat fingerprints from the right hand, four flat fingerprints from the left hand, and then simultaneous capture of the two thumbs; and (b) the "four-slap process," which requires four flat fingerprints from the right hand, and the right thumbprint, then four flat fingerprints from the left hand, and the left thumbprint. Once an individual's 10 fingerprints are collected and stored in IDENT, subsequent encounters, in most cases, will require the collection of fewer than 10 fingerprints for purposes of verification.

1.5 How will the information be checked for accuracy?

The collection of up to 10 fingerprints rather than 2 fingerprints will improve the likelihood of matching against fingerprints of known persons as well as latent prints (i.e., full or partial fingerprints of unknown persons, such as from a bomb fragment) when establishing and verifying an individual's identity, since there are more fingerprints with which to compare. The additional fingerprint data will improve IDENT's interoperability with other government databases, while reducing the time needed to determine an individual's potential security risk or eligibility to receive a benefit.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The statutory authority for the collection of biometrics from those individuals entering and exiting the U.S. includes, but is not limited to, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, (USA PATRIOT Act); the Homeland Security Act of 2002; the Enhanced Border Security and Visa Reform

Act of 2002 (Border Security Act); and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). See 8 U.S.C. §§ 1365a *note*, 1365b.

In addition, the data maintained in IDENT are collected based on program authorities for each agency collecting the data from individuals. These authorities are described in the PIAs, SORNs, or other materials published by each program.

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

Anytime biometric data (fingerprints, digital photograph) and biographic data (textual expressions of name, gender, date of birth) are collected, there is a risk of unauthorized access and disclosure. In order to mitigate privacy risks inherent in the collection of personally identifiable information, DHS employs physical, technical, and administrative security controls. These controls are validated through a Certification and Accreditation process on a regular basis. Users have limited access based on their roles and are trained in the proper handling of personally identifiable information. The infrastructure behind US-VISIT will not be changing significantly to accommodate the collection of more fingerprints, so access to, and security of, additional information will follow currents procedures (see Section 8.0 herein). US-VISIT's privacy program will continue to ensure the protection of all collected data.

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.

There will be no change to the uses of data collected by US-VISIT from foreign nationals as described in previous PIAs. This information will be used to identify and verify an individual's identity in the course of determining whether the alien is admissible, eligible for a benefit, and otherwise in lawful status.

2.2 What types of tools are used to analyze data and what type of data may be produced?

There is no change from previous PIAs as to the type of analysis tools used or the type of analysis performed. The collected data will be matched against DHS and other mission-related federal government databases to identify potential immigration or criminal impediments to

admission, or receipt of a benefit. The results of any analysis done on collected fingerprints and biographic data are used to identify or verify an individual's identity in determining admissibility to the U.S., eligibility for a benefit, or continued lawful status (e.g. analysis to determine whether the alien poses a criminal or national security threat).

2.3 If the system used commercial or publicly available data please explain why and how it is used.

US-VISIT does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Described any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

There are no changes from previous PIAs as to the controls in place to ensure that the information is appropriately handled. The 10 fingerprints will be used in the same way and for the same purposes as the 2 fingerprints. DHS employs physical, technical, and administrative security controls that are validated through a Certification and Accreditation process on a regular basis. Users have limited access based on their roles and are trained in the proper handling of personally identifiable information.

Section 3.0 Retention

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

3.1 How long is information retained?

In accordance with the IDENT System of Records Notice (SORN), biometric and biographic data are treated the same for retention purposes. These data will be retained no longer than 75 years.

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

The retention schedule for IDENT has been approved by NARA.

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

There is no change to reasons governing the retention period for data in IDENT based on the collection of 10 rather than 2 fingerprints. IDENT data is retained for the minimal period necessary to carry out DHS' national security, law enforcement, immigration, intelligence and other mission-related functions.

Section 4.0 Internal Sharing and Disclosure

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

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

The internal organizations with which US-VISIT shares data will remain the same in its 10 fingerprint collection.

As a primary DHS-wide repository of biometrics, and specifically as the holder of US-VISIT data, IDENT data is currently shared with components throughout DHS (e.g., United States Citizenship and Immigration Services, United States Customs and Border Protection, and Immigration and Customs Enforcement). US-VISIT shares the data contained in IDENT for DHS national security, law enforcement, immigration, intelligence, and other 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.

4.2 How is the information transmitted or disclosed?

When data are transmitted between IDENT and other systems on the DHS core network, it is done on an unclassified, secured wide area network. Other types of transmission or disclosure may be required in some circumstances. The mode of transmission or disclosure for each program will be done in accordance with DHS policy, regulation and, if applicable, under the terms of an agreement executed between the parties.

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

As there is no change to internal sharing of data based on the transition from 2 to 10 fingerprints, there is no change to the privacy risks from those described in previous PIAs. In many cases data sharing within DHS is required by statute, regulation, or Executive Order. In all cases, however, this data must be kept secure, accurate, and appropriately controlled. US-VISIT ensures that any privacy risks are mitigated through auditing access controls, re-sharing limits (where appropriate), and other physical, technical, and administrative controls.

Section 5.0 External Sharing and Disclosure

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

5.1 With which external organization(s) is the information shared, what information is shared, and for what purposes?

The external organizations with which US-VISIT shares data is not changed. US-VISIT will share 10-fingerprint data with the same organizations that it shares any other type of IDENT data, such as Federal, state, local, tribal, foreign, or international government agencies engaged in national security, law enforcement, immigration, intelligence, and other mission-related functions. For instance, data will be shared with the FBI for purposes of identifying known or potential criminals and terrorists.

All such external sharing will be subject to applicable laws, regulations, and memoranda of understanding (MOU), business rules and any other appropriate restraints on external data sharing.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS?

The sharing of 10-fingerprint data supports the purpose for the original collection as stated in the IDENT SORN, which is to enable DHS to carry out its national security, law enforcement, immigration, intelligence, and other mission-related functions, and to provide associated testing,

training, management reporting, planning and analysis, and other administrative uses, by allowing DHS to either confirm or reject an individual's claimed identity by comparing biographic and biometric information associated with the individual.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Ten-fingerprint data will be 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
- Secure transfer, including encryption on portable media, where there is no direct connection between systems.

The mode of transmission or disclosure for each program will be described in an MOU or other data sharing agreement associated with that particular program.

DHS enters into MOUs or other agreements with all non-DHS organizations with which information from IDENT is shared. These agreements provide the conditions for sharing or disclosing information, including governing the protection and use of the information.

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

As there is no change to external sharing of data based on the transition from 2 to 10 fingerprints, there is no change to the privacy risks from those described in previous PIAs. Data shared with external organizations must be kept secure, accurate, and appropriately controlled. US-VISIT ensures that any privacy risks are mitigated through data sharing agreements, which require 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 of the collection is provided by the publication of this PIA and the IDENT SORN, as updated (72 FR 3180, June 5, 2007). In addition, notice is provided at international arrival lanes equipped with fingerprint scanners capable of capturing 10 fingerprints, and through a variety of outreach efforts.

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

Foreign travelers covered by the Program and arriving to the U.S. are currently required to provide 2 fingerprints for verification purposes prior to being admitted to the country. If an individual refuses to provide the required amount of fingerprints, then he/she may be sent for further inspection and entry may be denied. This remains true for those individuals from whom 10 fingerprints rather than 2 fingerprints are collected. This process is necessary due to the national security, law enforcement, immigration, intelligence, and other DHS-mission related purposes underlying the collection of fingerprints from foreign nationals arriving to the United States.

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

Up to 10 fingerprints are collected from all individuals covered by US-VISIT. Because of the border management purposes of this collection, individuals will have no right to consent to a particular use of their data.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided through the publication of this PIA and the IDENT SORN. The 10-fingerprint data are collected with the knowledge of the individual for the purposes of national security, law enforcement, immigration, intelligence, and other DHS-related missions. In most cases, individuals do not have any right or opportunity to refuse providing this data or consenting to its particular uses.

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 transition from 2 to 10 fingerprint collection does not alter the procedures used by an individual to access his/her information contained in IDENT.

US-VISIT information may, in some cases, 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. In those cases, access to 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 many other cases, individuals may request and receive access by submitting a request to the Privacy Officer, US-VISIT Program, U.S. Department of Homeland Security, Washington, DC 20528.

7.2 What are the procedures for correcting erroneous information?

The transition from 2 to 10 fingerprint collection does not alter the procedures for an individual to correct erroneous information contained in IDENT. Individuals may have an opportunity to correct their data when it is being collected; otherwise, they may submit a redress request to the Traveler Redress Inquiry Program (TRIP) at WWW.DHS.GOV/TRIP or via mail, facsimile or email in accordance with instructions available at WWW.DHS.GOV/TRIP.

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

Redress procedures are established and operated by DHS through Traveler Redress Inquiry Program which can be contacted at WWW.DHS.GOV/TRIP.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

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.

Redress is provided through TRIP. While the system that contains the fingerprints, IDENT, does exempt some rights of access, this is done on a case-by-case basis. For instance, access may not be provided to those under criminal investigation. In the vast majority of cases, access and redress are provided. It is in the best interest of US-VISIT to ensure that the data are as accurate as possible, so that appropriate decisions may be made using this data.

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?

DHS personnel and contractors will have access to US-VISIT data as described in previous PIAs. The primary user groups include CBP officers, system managers, developers, and analysts. Access will be limited to the extent required for the particular user group to complete their responsibilities.

8.2 Will Department contractors have access to the system?

Contractors will have access to US-VISIT 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 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All government employees and contractors are required to complete privacy training when they initially join the US-VISIT program. Subsequent yearly privacy refresher training is required of all government employees and contractors on US-VISIT.

8.4 Has Certification & Accreditation been completed for the system or system supporting the program?

IDENT was granted an authority to operate in May 2007, this authority to operate will expire in May 2010, unless reaccreditation takes place beforehand.

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

US-VISIT 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), as described in previous PIAs.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Anytime biometric data (fingerprints, digital photograph) and biographic data (textual expressions of name, gender, date of birth) are collected, there is a risk of unauthorized access and disclosure. However, the change from collecting 2 to collecting 10 fingerprints does not affect the existing technical access and security controls protecting that data. In order to mitigate privacy risks inherent in the collection of personally identifiable information, DHS employs physical, technical, and administrative security 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 roles. Users are also trained in the handling of personally identifiable information. The specific access controls for each use of information is described in the PIA relating to that use of information.

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?

IDENT and the 10-fingerprint capture devices are comprised of standard commercial hardware and software that has been modified to meet the needs of DHS.

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

Policy, operational, and technical aspects were extensively analyzed to ensure that data integrity, privacy, and security protections were preserved in the transition from the collection of 2 fingerprints to the collection of 10 fingerprints. US-VISIT uses a privacy risk management process based on information life cycle analysis and fair information principles. 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 mitigation approaches are developed.

9.3 What design choices were made to enhance privacy?

The design, development and implementation of all systems involved in the transition from the collection of 2 fingerprints to the collection of 10 fingerprints was assessed using a privacy risk management process that includes a PIA, and compliance with the IDENT SORN, applicable laws, regulations, guidance and best practices.

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

There are no significant technical changes to IDENT to support the transition from the collection of 2 fingerprints to the collection of 10 fingerprints. The major technical change is the

move to devices that collect 10 rather than 2 fingerprints, and these devices are continuously tested and upgraded to ensure that they provide the best service possible, while not compromising the privacy of the traveler.

Responsible Officials:

Barbara M. Harrison, Acting US-VISIT Privacy Officer
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security