Privacy Impact Assessment
for the

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

In conjunction with the Notice of Proposed Rulemaking on the Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure

April 15, 2008

Contact Point
Paul Hasson, Acting Privacy Officer
US-VISIT Privacy Office
(202) 298-5021

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

Abstract

The United States Visitor and Immigrant Status Technology (US-VISIT) Program is implementing the first phase of the Exit component of its integrated, automated biometric entry-exit system that records the arrival and departure of covered aliens; conducts certain terrorist, criminal, and immigration violation checks of covered aliens; and compares biometric identifiers to those collected on previous encounters to verify identity. The US-VISIT Program has been implemented in phases with each phase adding additional capabilities, locations of implementation, or subject populations. US-VISIT is publishing this Privacy Impact Assessment (PIA) in conjunction with the Notice of Proposed Rulemaking (NPRM) on Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure. A revised PIA will be issued in conjunction with the Final Rule on Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure. US-VISIT does not collect any information on United States citizens.

Overview

US-VISIT records the arrival and departure of covered aliens[1]; conducts terrorist, criminal, and immigration violation checks on covered aliens; and compares biometric identifiers to those collected on previous encounters to verify identity. US-VISIT has been implemented in phases beginning with an entry and a pilot exit program and expanding to additional capabilities, locations of implementation, or subject populations[2]. The Exit NPRM and this PIA address a substantial deployment of the US-VISIT biometric Exit capability for international departure from air and sea ports.

The NPRM proposes that US-VISIT implement a full Exit Program in accordance with its statutory mandate of the Immigration and Nationality Act (INA) §§ 215, 231, 262(a), 263(a), 264(c), 8 United States Code 1185, 1231, 1302(a), 1303(a), 1304(c), Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208, the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; the U.S.A. PATRIOT Act, Public Law 107-56; the Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173; the Intelligence Reform and Terrorism

1 Reference to covered aliens includes all visiting, non-immigrant aliens, or visiting non-United States Citizens as identified under US-VISIT requirements, and section 2. System Overview, of the US-VISIT Program. There is no change to the aliens subject to US-VISIT requirements. For more information, read the most recent Privacy Impact Assessment for the US-VISIT Program (available at www.dhs.gov/privacy, follow link to "Privacy Impact Assessments"). .

2 US-VISIT does not intentionally collect information on United States citizens

Prevention Act of 2004, Public Law 108-458; and the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, and many other statutes. According to the NPRM carriers at air and sea ports of international departure will collect limited biographic and biometric information from covered aliens, and transmit the biographic and biometric information to the Department of Homeland Security (DHS).

Because the NPRM expressly solicits comments on the proposed Rule, the exact details of the implementation of the Exit Program are not known. However, certain basic facts are known. The Exit Program will require biometric information and a minimal amount of biographic data, not to exceed the equivalent of the biographic information available in the machine-readable zone of a travel document. The carriers will collect the biographic and biometric information prior to covered aliens boarding for an international departure. The carriers will then package this personally identifiable information (PII) and transmit it to DHS, using standards provided by DHS. Once the PII is received by DHS, DHS will acknowledge receipt to the carrier. The receipt will not contain any PII or instruction back to the carrier regarding the covered alien.

When the required biographics and biometrics are received by DHS, US-VISIT Entry/Exit matching will take place. US-VISIT will biometrically verify the identity of previously encountered covered aliens departing the United States as required by the INA and the NPRM. US-VISIT will also conduct a biometric check against a list of subjects of interest. Results of this biometric check will be referred to and managed by the appropriate DHS agencies on a case by case basis. Biometrics that match a covered alien's US-VISIT record will be associated with that record and stored in the Automated Biometric Identification System (IDENT). When the identity of a covered alien cannot be biometrically verified against a previous encounter, the biometric will be stored in IDENT but it will not be associated with a previously collected covered alien's IDENT record. The biographics associated with the departing covered alien will be stored in the Arrival and Departure Information System (ADIS), regardless of whether there is a biometric match.

Carriers will be liable for penalties on an individual basis for failing to create and transmit a biometric departure record for covered aliens, as biometric submissions will be required by regulation to be part of the passenger manifest, and for inadequate transmission performance.

Moreover, carriers are not allowed to retain the biometric data or use the biometric data for purposes other than those outlined by US-VISIT in the standards guidance for carrier systems, which will be issued by DHS in conjunction with the Final Rule. It is DHS' expectation the carriers will follow the requirements listed in the standards guidance.

DHS and US-VISIT are publishing this PIA along with the NPRM to outline the potential privacy impact of the Exit Program. Although not all details of the Exit Program are known, this PIA serves to discuss the privacy impact of the known structure of the program. A PIA update that

analyzes the privacy impact of the implementation of the Exit Program will be published concurrently with the Final Rule.

Section 1.0 Characterization of the Information

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

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

US-VISIT Exit processing will require the collection of biometric data and biographic data[3]. Since carriers already collect biographic data for use in the Customs and Border Protection's (CBP) Advance Passenger Information System (APIS) and Transportation and Security Administration's (TSA) Secure Flight Program, the collection of this data will not change.[4] The only change will be the additional collection of biometrics.

In order to minimize data collection and transmission, US-VISIT will collect a minimal amount of biographic data, not to exceed the equivalent of the biographic data stored in the machine-readable zone of a travel document. The biographic data is necessary, and must be sufficient, in order to associate the biometrics with the total set of biographic information collected for the APIS manifest requirements. The carrier will then send the biometric data and the minimal biographic data to DHS, whereupon DHS will acknowledge receipt to the carrier. The receipt will not contain any PII or instruction back to the carrier regarding the covered alien.

Once the required biographics and biometrics are received by DHS, US-VISIT Entry/Exit matching will take place. US-VISIT will conduct a biometric check against a list of subjects of interest. Results of this biometric check will be referred to and managed by the appropriate DHS agencies on a case by case basis. US-VISIT will also verify the identity of a covered alien previously encountered by comparing the Exit biometric data to the biometric data in their US-VISIT record. The biometrics that match a covered alien's US-VISIT record will be associated with that record and stored in IDENT. When the identity of a covered alien cannot be biometrically verified against a previous encounter, the biometric will be stored in IDENT, but it will not be associated with a previously collected covered alien's IDENT record. However,

[3] In some cases, a unique identifier may be used to align the biometric data and the biographic data together. Regardless, the minimal biographic data, and not the unique identifier, enables IDENT to match biometrics.
[4] APIS is a module of the Treasury Enforcement Communications System (TECS) owned and operated by Customs and Border Protection (CBP) of DHS.

US-VISIT will maintain a biographic record of the covered alien's departure, and this biographic record of departure will be associated with the covered alien's record located in ADIS.

The data collected during US-VISIT Exit will be retained in three DHS systems. The biometric and biographic data are retained in IDENT. The majority of the biographic data and data associated with the actual encounter, including the identifier associated with a biometric, will be retained in ADIS. The biographic data required for CBP purposes is sent to APIS. In an effort to eliminate unnecessary duplication of carrier efforts to support other federal agency programs, US-VISIT Exit will align with CBP's APIS.

The data elements from IDENT, ADIS, and APIS are identified in the following table.

	IDENT	ADIS	APIS
Complete Name	X	X	X
Date of Birth	X	X	X
Citizenship	X	X	X
Sex	X	X	X
Travel Document Information	X	X	X
FingerprintID Number	X	X	X
Subjects of interest list Match	X	X	X
Nationality			X
Carrier Code		X	X
Vessel Port		X	X
Vessel Name		X	X
PNR Number		X	X
Arrival Information		X	X
Departure Information		X	X
USDestination Address		X	X
Passenger Status		X	X
Class of Admission		X	X

	IDENT	ADIS	APIS
Admit until date		X	X
Country of residence			X
Visa Information		X	X
Passport Information			X
A-Number			X
A-Number		X	X
Photograph	X		
Fingerprints	X		

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

US-VISIT covered aliens will provide biometrics to carriers during the departure process. Carriers will couple the biometrics with a minimal set of biographic data and transmit this data to US-VISIT via DHS. Additionally, the biographic data on the covered alien will come directly from APIS.

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

The collected PII is used to record the departure of covered aliens; conduct terrorist, criminal, and immigration violation checks on covered aliens; and to compare biometric identifiers to those collected on previous encounters to verify identity. For example, an immigration violation check could involve a covered alien who fails to comply with the US-VISIT departure process, whether intentionally or not. If their departure is not recorded, then that covered alien would risk being identified as overstaying their period of admission. US-VISIT and Immigration and Customs Enforcement (ICE) would investigate the status of the covered alien, and if it is determined that the alien has overstayed their period of admission, the covered alien could be subject to removal proceedings or denied entry to the U.S. during subsequent travel.

1.4 How is the information collected?

Carriers will collect the covered alien's biometrics using a biometric collection device that meets the technical specifications identified by US-VISIT. The biometric collection device must comply with the Integrated Automated Fingerprint Identification System (IAFIS) Image Quality

Specifications. Data transmission will take place over an encrypted network between the carrier industry and DHS. The encrypted networks must comply with the standards set forth in the Interconnection Security Agreements (ISAs) required to be executed prior to external access to DHS systems.

1.5 How will the information be checked for accuracy?

Carriers are responsible for the accuracy of the biometric data captured from the covered alien and any other transmitted data. The following protection strategies will be used to ensure the accuracy of the biographics and biometrics.

- Carriers will collect the biometrics directly from the covered alien.
- Carriers will comply with DHS standards for the secure storage and transmission of the biographics and biometrics.
- Carriers will comply with the IAFIS Image Quality Specifications.
- Carriers will comply with DHS standards for purging their systems of PII secured for and transmitted to US-VISIT.
- Carriers will immediately notify the Privacy Officer of US-VISIT in writing in event of unauthorized use or access, or breach of biometric departure manifest information.
- Carriers will register their carrier system with DHS, and registration will be contingent upon compliance with standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule.
- US-VISIT will only retain those data elements, which are required to be submitted for the purposes of US-VISIT Exit processing.
- US-VISIT quality assurance processes will identify any errors concerning properly matching covered aliens with relevant records, e.g., special checks to ensure the quality of submissions by the carrier, and human analysis to verify overstay records for possible law enforcement action.
- US-VISIT will maintain existing audit capabilities for the government systems supporting US-VISIT and may use auditing to ensure carrier systems comply with the standards guidance to be issued by DHS in conjunction with the Final Rule.
- US-VISIT will provide an opportunity for correcting inaccurate data through the DHS Traveler Redress Inquiry Program (TRIP), which is described in detail online at https://trip.dhs.gov.

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

The US-VISIT Program was authorized by, and finds its basis in, provisions of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208, the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; the Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; the U.S.A. PATRIOT Act, Public Law 107-56; the Enhanced Border Security and Visa Entry Reform Act ("Border Security Act"), Public Law 107-173; and the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458. Also, and most recently, Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338 the Secure Travel and Counterterrorism Partnership Act of 2007 (STCPA) directs the Secretary of Homeland Security, within one year of enactment, to "establish an exit system that records the departure on a flight leaving the United States of every [covered] alien participating in the visa waiver program…." This exit system must match biometric information against relevant DHS lists of subjects of interest and immigration information; and compare such information against manifest information collected by air carriers on passengers departing the United States to confirm such covered aliens have departed the United States.

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

Carrier collection of PII creates the vulnerability that carriers may use the PII for purposes other than those required by US-VISIT and thereby misuse the PII. For example, carriers may violate standards established by US-VISIT and use the PII without authorization from US-VISIT to achieve business process efficiencies or to profit from the sale of the PII to third parties. Moreover, with carrier custody of PII, the government has less confidence that the PII is being collected and handled in accordance with applicable laws, regulations, policies, and fair information principles. The potential threats to privacy include:

- Inadequate security by the carrier—Carriers may create a new repository of PII on carrier systems that is vulnerable to unauthorized access, use, disclosure and retention;
- Inadequate data integrity—Biometrics captured by the carrier may not be of sufficiently high quality to allow for appropriate matching; biometrics may be modified without authorization while in carrier custody;
- Inadequate identification of purpose—Carriers may misrepresent how the biometrics collected from the covered alien may be used, e.g. carriers may fail to distinguish adequately between mandatory government use of biometrics and a commercial business use such as a carrier's registered traveler program; and

- Inadequate openness and transparency—Carriers may not provide sufficient details to allow covered aliens to understand how their information will be used.

As it relates to US-VISIT processing, the impact of these threats on the covered alien could include potential travel inconvenience or delays, possible subsequent denial of admission to the United States based on faulty data, or misuse of PII. As it relates to carrier collection of biometrics, the impact of these threats on the covered alien can include the loss of control over the use and disclosure of their PII. The opportunities for the misuse of PII, and the serious impact that carrier misuse would have on covered aliens and the integrity of the US-VISIT Program makes the misuse of biometrics by carriers a high risk.

US-VISIT seeks to address these risks in the NPRM, and ultimately the Final Rule, by minimizing the collection and transmission of PII where possible. The collection of fingerprints is necessary to meet the biometric requirements placed on the US-VISIT Program by statute. The collection of biographic information is necessary to facilitate the biometric identity verification and biometric check against DHS lists of subjects of interest.

US–VISIT will also seek to establish technical, security and privacy requirements in standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule. One purpose of these requirements is to restrict carrier use and retention of biometrics to the purposes stated by US–VISIT and to ensure that the PII is collected and handled in accordance with the fair information principles. Accordingly, US–VISIT is considering, and soliciting comment in the NPRM, on the use of encryption upon collection to secure the biometrics against unauthorized use, disclosure, and modification while the biometrics reside on carrier systems, and on whether to mandate that carriers provide notice that they are collecting biometrics on behalf of US-VISIT. Without clear restrictions on carrier use and retention of biometrics, the risks of carrier misuse and decreased data integrity will remain high. DHS expects that the carriers will follow the requirements listed in the standards guidance. However, to mitigate the risk effectively, an audit capability to ensure compliance with the restrictions may be necessary. A PIA will accompany the Final Rule and will assess the degree to which the requirements in the standards guidance for carrier systems are able to reduce the privacy risks associated with the Exit Program.

After US-VISIT receives the necessary PII, processing procedures are designed to ensure that the covered alien's international departure is properly recorded in the government systems that support US-VISIT. As a result of such processing, US-VISIT is able to retrieve information associated with a covered alien's departure—through biographics, or biometrics or both—in the event that the biographic or biometric manifest submitted by the carrier is incomplete or the biometrics captured are not of high enough quality to match against a previous biometric encounter stored in IDENT.

Furthermore, US VISIT protects the PII used for Entry/Exit processing through a robust Privacy and Security Program. As discussed in the January 5 and August 31, 2004 interim rules, US-VISIT records will be protected consistent with applicable privacy laws and regulations, including DHS' published privacy policy for US-VISIT.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

US-VISIT stores and uses the data collected during the Exit process to record the departure of covered aliens, conduct certain terrorist, criminal, and immigration checks on lists of subjects of interest on covered aliens, and compare biometric identifiers to those collected on previous encounters to verify identity. Results of the biometric check on lists of subjects of interest will be referred to and managed by the appropriate DHS agency on a case-by-case basis. US-VISIT will also verify the identity of a covered alien previously encountered by comparing the Exit biometric data to the biometric data in their US-VISIT record. The biometrics that match a covered alien's US-VISIT record will be associated with that record and stored in IDENT. When the identity of a covered alien cannot be biometrically verified against a previous encounter, the biometric will be stored in IDENT, but it will not be associated with any previously collected covered alien's US-VISIT record. Biometrics that cannot be matched to a US-VISIT record will not be enrolled in US-VISIT.

Carriers are not allowed to use the biometrics for any purpose other than those purposes stated by US-VISIT in standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule. It is DHS' expectation that the carriers will follow the requirements listed in the standards guide.

DHS proposes to conduct operational testing with carriers to verify the carrier's ability to package and transmit minimal biographics and biometrics to DHS that will be outlined in technical specifications and guidance. The testing will use fictitious biometric and biographic data to limit the risk associated with using PII.

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

US-VISIT will use tools to match entry and exit records and identify covered aliens overstaying their terms of admission. The results of US-VISIT matching will be analyzed for quality assurance purposes to improve matching algorithms. US-VISIT will also analyze subject-based patterns and in some cases will act upon that analysis to prevent immigration and law enforcement violations. Such analysis includes the identification of trends, which is essential to assessing risk and to enhancing the integrity of the immigration and border management system.

For example, trend analysis might reveal to DHS and Department of State specific visa-issuing posts, visa categories, VWP countries, or other locations or factors reflecting an unacceptably high overstay rate, allowing opportunities for self-assessment and more focused enforcement, including increased scrutiny of immigration benefit or visa renewal applications.

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

The Exit Program does not propose to add any commercial or publicly available data that is not already used by US-VISIT. US-VISIT may use publicly available data to confirm previously collected information and to assist in identifying the address or phone number of a covered alien. Public records are not relied on as the sole determinative information in any analysis or inquiry.

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

Collection of PII by carriers increases the risk that the data may be used for purposes other than those stated by US-VISIT. In addition, an individual who gains access to the carrier's system, whether authorized or not, might be able to use, analyze, disclose, modify, or retain the PII in unauthorized ways. Therefore, without clear restrictions on carrier use and retention of biometrics, the risk of misuse of biometrics by the carrier remains high.

To secure the PII against misuse and protect data integrity, DHS will establish technical, security and privacy requirements for the carrier systems submitting PII to US-VISIT in standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule. It is DHS' expectation that the carriers will follow the requirements listed in the standards guide. As currently proposed, the biometrics collected must comply with the IAFIS Image Quality Specifications. The biometrics and biographics (or unique identifier) submitted to DHS will be transmitted over an encrypted network, which complies with standards set forth in CBP's ISAs and

supports other electronic manifest data submissions. If carriers experience unauthorized use or access, or breach of biometrics or biographics supporting US-VISIT, carriers must immediately notify the US-VISIT Privacy Officer in writing. Moreover, US-VISIT is considering, and soliciting comment in the NPRM, the use of encryption upon collection to secure the biometrics against unauthorized use, disclosure and modification while the biometrics reside on carrier systems.

PII maintained by US-VISIT will in some cases be supplemented with public source data, which may be used by US-VISIT for limited data verification or establishing an address or phone number. This public source data presents particular issues because this type of data is prone to lack currency and correctness. However, these data elements are not, in and of themselves, used for making decisions about covered aliens. In addition, all PII maintained by US-VISIT will be protected against unauthorized use, modification, and/or retention by a robust privacy and security program. As discussed in the January 5 and August 31, 2004 interim rules for the US-VISIT Program, US-VISIT records will be protected consistent with all applicable privacy laws and regulations, including DHS' published privacy policy for US-VISIT. Physical, technical, and administrative controls, which include access controls and system user education and training, will keep PII secure and confidential. PII collected by US-VISIT will not be discussed with, nor disclosed to, any person within or outside US-VISIT other than as authorized by law and as required for the performance of official duties. A program-dedicated Privacy Officer ensures that the data is not used or accessed improperly and the DHS Chief Privacy Office continues to exercise oversight of US-VISIT to ensure that the information collected and stored in IDENT and other systems associated with US-VISIT is being properly protected under current privacy laws and guidance.

The US-VISIT security policy, discussed further in Section 8.0, requires that the confidentiality and security of an individual's personal information be maintained. Accordingly, the three primary systems supporting US-VISIT are validated through a Certification and Accreditation process on a regular basis. US-VISIT is the system owner for IDENT and ADIS, and CBP is the system owner for APIS. IDENT was granted an authority to operate in May 2007 and that authority to operate will expire in May 2010. ADIS was granted authority to operate in October of 2006 and that authority will expire in October of 2009. APIS (via TECS) was granted authority to operate in January of 2006 and that authority will expire January of 2009. These authorities to operate will be subject to renewal prior to expiration. As mentioned above, users of these systems have limited access that is established based on their roles and are trained in the handling of personal 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?

US-VISIT will restrict carriers' retention of biometric data in standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule. It is DHS' expectation that the carriers will follow the requirements listed in the standards guide.

Upon receipt by DHS, the minimal biographics and the biometrics will be retained in accordance with the Systems of Records Notices (SORNs) published for the systems that support US-VISIT. The retention periods for IDENT and ADIS is 75 years or until the statute of limitations has expired for all criminal violations. Data stored in CBP's APIS will be maintained for as long as operationally necessary, subject to retention reviews that occur both periodically, and each time information is accessed, but in no case will information be retained longer than 50 years past the date of collection.

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

The retention schedule for IDENT, ADIS, and APIS has been approved by NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Given that carriers collect PII on behalf of US-VISIT, there is a risk that a persistent biometric database, vulnerable to unauthorized use and disclosure, could be created. To reduce this risk, US-VISIT seeks to minimize the amount of PII collected.

US-VISIT will also establish technical, security and privacy requirements in standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule. One purpose of these requirements is to restrict carrier use and retention of biometrics to the purposes stated by US−VISIT and to ensure that the PII is collected and handled in accordance with the fair information principles. Accordingly, US-VISIT is considering, and soliciting comment in the NPRM, the use of encryption upon collection to secure the biometrics against unauthorized use, disclosure, and modification while the biometrics reside on carrier systems. Without clear

restrictions on carrier use and retention of biometrics, the risk of misuse of biometrics by the carrier is high. It is DHS' expectation that the carriers will follow the requirements listed in the standards guide. However, to mitigate the risk effectively, an audit capability to ensure compliance with the restrictions may be necessary. A PIA will accompany the Final Rule and will assess the degree to which the requirements in the standards guidance for carrier systems are able to reduce the privacy risks associated with the Exit Program.

Once received by DHS, the PII will be retained in accordance with the SORNs for the systems that support US-VISIT. US-VISIT's systems IDENT and ADIS have a retention period of 75 years; APIS has a retention period of no longer than 50 years. The difference in retention periods raises some risk of inconsistency and duplication that can result in some heightened degree of integrity/security, access, and/or redress risk, as personal information could be deleted from one or more component systems while being retained in others. However, the retention periods are dependent on the varied purposes and needs of different system owners.

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 purpose?

The biometrics and corresponding biographics received by US-VISIT during Exit processing may be shared, upon request, with appropriate Federal, state, local, tribal, foreign, or international Governmental agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for purposes of national security, law enforcement, immigration, intelligence, and other mission-related functions as determined by the Secretary, and as otherwise authorized by law. Data maintained by US-VISIT in service of its entry-exit system is shared principally with staff of DHS components engaged in immigration and border security—CBP, ICE, and Citizenship and Immigration Services. However, US-VISIT may occasionally share data with other DHS organizations on a systematic, non-routine use basis, such as the United States Coast Guard (USCG) for similar purposes. The sharing activities for Exit biometrics and corresponding biographics are consistent with data sharing and internal disclosures previously identified for the US-VISIT Program[5].

[5] For more information on how information can be shared internal to DHS, see the Systems of Records Notices (SORNs) for the systems that support US-VISIT: IDENT SORN, DHS/USVISIT-0012, June 5, 2007, 72 FR 31080 < http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/E6-11995.htm>; ADIS SORN, DHS/USVISIT-001, August 22, 2007, 72 FR 47057 <http://www.dhs.gov/xlibrary/assets/privacy/privacy_sorn_usvisit_adis.pdf>; and TECS/APIS DHS/CBP-005,

4.2 How is the information transmitted or disclosed?

The biometrics and corresponding biographics will be shared only in accordance with the duly published SORNs for systems supporting US-VISIT. When authorized, US-VISIT data can be shared via dedicated T1/T3 lines, extracts on encrypted mobile devices, and ISA-covered connections. Any transmission or disclosure conducted by US-VISIT in accordance with a Letter of Intent (LOI) or Memorandum of Understanding (MOU) will have transmission and security requirements established in the authorizing documents.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

There are no additional disclosures or internal data sharing from the US-VISIT Program as a result of the proposed rule.

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. US-VISIT mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are documented in sharing agreements.

In all cases of sharing internal to DHS, all components are required to comply with the Department's security policies and procedures, 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, which are applied to component systems, communications between component systems, and at all interfaces between component systems and external systems. For example, external connections must be documented and approved with both parties signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

US-VISIT satisfies all the DHS security requirements and each of its systems have been certified and accredited. As other DHS components meet the security requirements and their systems that support US-VISIT receive certification and accreditation, an additional layer of security protection is added to the US-VISIT program.

August 23, 2007, 72 FR 48349
<http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-15976.htm>.

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 purpose?

There are no additional disclosures or external data sharing from the US-VISIT Program as a result of the proposed rule. Data received by DHS from carriers does not constitute data sharing. Carriers are considered collection agents. US-VISIT will not share any PII with the carrier. The only information provided by US-VISIT to the carrier is the acknowledgement that the PII has been received; the acknowledgement will not contain any PII.

US-VISIT shares biometrics and corresponding biographics with other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders.

The SORNs for the source systems on which US-VISIT draws provide notice as to the routine uses for the information collected by US-VISIT, provided that any disclosure is compatible with the purpose for which the information was collected.

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 biometrics and corresponding biographics outside the DHS is compatible with the purposes of collection and is covered by the routine uses listed in the SORNs for the systems that support US-VISIT. Moreover, DHS has entered into MOUs or other agreements with non-DHS organizations with which US-VISIT shares information. These agreements provide the conditions of sharing or disclosure, including how the information must be protected and how it can be used.

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

Once the biometrics and corresponding biographics are received by US-VISIT and integrated with the US-VISIT Program, the data will be shared only in accordance with the duly published SORNs for systems supporting US-VISIT. When authorized, US-VISIT data can be shared using dedicated T1/T3 lines, extracts on encrypted mobile devices, and ISA-covered connections. Any transmission or disclosure conducted by US-VISIT in accordance with a LOI or MOU will have transmission and security requirements established in the authorizing documents.

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

There are no additional disclosures or external data sharing from the US-VISIT Program as a result of the proposed rule. Data received by DHS from the carrier does not constitute data sharing. Carriers are considered collection agents of US-VISIT and DHS. The only information provided by US-VISIT to the carrier is the acknowledgement that PII has been received; the acknowledgement will not contain PII.

Any data sharing, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. US-VISIT mitigates these vulnerabilities by working closely with the sharing organizations to establish formal agreements and develop secure standard operating procedures for sharing the data. Furthermore, US-VISIT complies with the DHS comprehensive program for information security. The security program involves the establishment of strict rules of behavior for each major application, including US-VISIT. It includes a periodic assessment of physical, technical, and administrative controls designed to enhance accountability and data integrity. It also requires that all users be adequately trained regarding the security of their systems, that system users must participate in a security training program, and that contractors and consultants must also sign a non-disclosure agreement. External connections must be documented and approved with both parties signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

Section 6.0 Notice

The following questions are directed at notice to the covered alien 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?

Notice will be provided by this PIA update and corresponding NPRM, and the US-VISIT website. US-VISIT is also considering whether to require carriers to provide notice explaining that the carrier is collecting PII on behalf of US-VISIT, how US-VISIT will use the PII, and the effect of not providing the PII. DHS seeks comment in the NPRM on how a privacy notice could be provided prior to collection of biometrics.

Additional notice and public education may be conducted by US-VISIT if this is deemed necessary based on public comments received on the publication of the PIA and NPRM.

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

Covered aliens do not have the right to decline to provide information and still depart the United States. Under the authority of 8 U.S.C. 1221 and 49 U.S.C. 44909, and Section 711 of the Secure Travel and Counterterrorism Partnership Act of 2007, US-VISIT mandates the collection of PII to record the arrival and departure of covered aliens, conduct certain terrorist, criminal, and immigration violation checks of covered aliens, and compare biometric identifiers to those collected on previous encounters to verify identity.

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

Covered aliens do not have the right to consent to particular uses of the information as US-VISIT is required to record the arrival and departure of covered aliens, conduct certain terrorist, criminal, and immigration violation checks of covered aliens, and compare biometric identifiers to those collected on previous encounters to verify identity. As described in previous US-VISIT PIAs, the PII collected on behalf of US-VISIT is used only for the purposes of border and immigration management, national security, and law enforcement.

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.

US-VISIT relies on notice to mitigate the privacy risks posed by mandatory collection and use of PII. Transparency created by US-VISIT PIAs, NPRMs and Final Rules, and public education efforts ensures that covered aliens understand what information will be collected and how it will be used.

Because carriers are acting on behalf of US-VISIT, however, there is a risk that covered aliens will not understand that US-VISIT will be using their PII, and not the carriers. To reduce this risk, US-VISIT is considering, and soliciting comments in the NPRM, whether to mandate carriers notify covered aliens that the carrier is collecting biometrics on behalf of US-VISIT prior to collection.

Section 7.0 Access, Redress and Correction

The following questions are directed at a covered alien's ability to ensure the accuracy of the information collected about them.

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

Individuals may gain access to their information held by US-VISIT by filing a request under the Freedom of Information Act (FOIA) or the Privacy Act of 1974, except where the disclosure of records or portions of a record are subject to narrow exceptions for criminal or other law enforcement purposes. A FOIA request must reasonably describe the specific records sought and must be made in accordance with US-VISIT's FOIA regulations. A reasonable description of DHS records would allow a DHS employee to locate records using reasonable efforts. For more information on submitting a FOIA request see "How to Submit a FOIA Request" at http://www.dhs.gov/xfoia/editorial_0316.shtm.

Individuals may also gain access to their information held by US-VISIT by filing a request under the Privacy Act of 1974. The Privacy Act grants U.S. citizens and Legal Permanent Residents (LPRs) the right to access and amend their records. DHS and US-VISIT policies extend these rights to US-VISIT covered aliens. Privacy Act requests of US-VISIT should be submitted to: US-VISIT FOIA Officer; Department of Homeland Security, Washington, DC 20528; Phone (202) 298-5200; Fax (202) 298-5201; US-VISIT-FOIA@dhs.gov.

7.2 What are the procedures for correcting inaccurate or erroneous information?

There are no changes to existing procedures for correcting inaccurate or erroneous information as a result of the proposed rule. Covered aliens will continue to have a redress process available to them to correct inaccurate or erroneous information held by the US-VISIT Program.

To correct inaccurate or erroneous information, covered aliens must submit a redress request through the DHS Traveler Redress Inquiry Program (TRIP) website, https://trip.dhs.gov. Once a covered alien submits a redress form, the individual will receive notification of receipt. DHS TRIP will review the redress form and determine which component/agency will most effectively be able to respond to the submission. When a redress request is related to US-VISIT processing, TRIP will coordinate with US-VISIT. US-VISIT will then review the covered alien's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution to their request.

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

Covered aliens are notified of the procedures for correcting their information through the NPRM for Exit, this PIA, and DHS and US-VISIT websites. The redress procedures are established and operated by DHS through TRIP, which can be accessed at https://trip.dhs.gov.

7.4 If no formal redress is provided, what alternatives are available to the individual?

If redress cannot be provided, or the covered alien is dissatisfied with the response received from US-VISIT, the individual can appeal their case to the DHS Chief Privacy Officer, who will review the appeal and provide final adjudication concerning the matter. The DHS Chief Privacy Officer can be contacted at Chief Privacy Officer, ATTN: US-VISIT Appeal, Department of Homeland Security, Washington, D.C. 20528, USA; or Fax: 00-1-202-772-5036.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

DHS TRIP provides a redress process that furthers the privacy interest of the covered alien by providing an easy-to-use website that provides a central point of contact for the submission and processing of redress requests. DHS TRIP collects PII directly from the individual, and therefore

the risk of collecting inaccurate information should be minimized. PII submitted to DHS TRIP will be protected, and will only be shared in accordance with the provisions of the Privacy Act of 1974 (5 U.S.C. § 552a) and as provided in the DHS TRIP Privacy Impact Assessment, published January 18, 2007. In addition, covered aliens may request access to or correction of their personally identifiable information pursuant to FOIA or the Privacy Act, as appropriate.

Section 8.0 Technical Access and Security

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

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

As proposed, US-VISIT Exit will rely on systems that are outside the direct control of the US government—the carriers systems—in addition to the government systems that already support the US-VISIT Program. Access procedures for carrier systems are dependent on the carrier. Access procedures for government systems have been established by the owners of those government systems. Carriers supporting US-VISIT Exit will not have direct access to government systems that support US-VISIT.

DHS has documented standard operating procedures to determine which users may access systems that support US-VISIT. To access these systems, users must hold the appropriate security clearance, perform a clearly defined role requiring access to the information in the system, and receive the mandatory security and privacy training. The clearance, job responsibilities, and mandatory security and privacy training activities for all individuals permitted access to US-VISIT systems are documented and maintained to reflect changes in user status and responsibilities. Access is then granted on the principles of least privilege, separation of duties, and need to know. A user's "need to know" depends on context of when, how and why the user requires access to information. Accordingly, "need to know" is asserted by the user after the other procedures to obtain access have been established, and that assertion is validated and confirmed by the user's manager, the system manager, and security personnel. Event logs record system access, and the Information System Security Manager (ISSM) confirms compliance to policy and manages the activation or deactivation of accounts and privileges as required or when expired.

The access control procedures operate in conjunction with a robust security program that implements physical, administrative, and technical controls to protect the confidentially, integrity and availability of the system.

8.2 Will Department contractors have access to the system?

In accordance with the access policies and procedures established by DHS for government-owned systems, contractors will have access to the systems that support the US-VISIT Program, including IDENT, ADIS, and APIS, to perform their official duties such as system administration, monitoring, and security functions. Contractor access will be granted in accordance with the principles of least privilege, separation of duties and need to know. The access policies and logs will be reviewed by security management to ensure the effective implementation of privacy and security safeguards.

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

Established US-VISIT Program privacy training requirements will address the needs of US-VISIT Exit as it relates to the government system users. All users of government systems supporting the US-VISIT Program receive privacy training prior to obtaining access to those systems. DHS personnel, including government personnel and contractors, are required to take mandatory privacy training offered by their DHS component. US-VISIT personnel receive an instruction on privacy regulations and legislation, the responsibilities of the US-VISIT Privacy Team, and the privacy rules of behavior governing the performance of professional duties. Users external to DHS, who are a party to data sharing arrangements, are also required to receive privacy training in accordance with the MOU or other agreement authorizing the sharing of data.

Carriers will not have access to DHS systems, including IDENT, ADIS, or APIS, and accordingly, will not receive privacy training for those systems.

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

As proposed, US-VISIT Exit processing will rely partially on systems that already support the US-VISIT Program and certification and accreditation has already been completed for those systems.

The three primary systems supporting US-VISIT are IDENT, ADIS, and the Passenger Processing Component of APIS. IDENT was granted an authority to operate in May 2007; this authority to operate will expire in May 2010. ADIS was granted an authority to operate in October of 2006; this authority to operate will expire in October of 2009. APIS was approved through TECS Certification and Accreditation in January 3, 2006.

Carrier systems will not be certified and accredited through the DHS process because carrier systems are not DHS owned systems.

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

The Exit Program does not propose to add any auditing measures that are not already used by US VISIT. However, to mitigate the risk of the misuse of biometrics effectively, an audit capability may be necessary to ensure compliance with the restrictions that will be established in standards guidance for carrier systems along with the Final Rule.

The PII received by DHS is subject to appropriate technical safeguards and audit capabilities of the systems in which the PII is stored. US-VISIT secures information, and the systems on which that information resides, by complying with the requirements of DHS information technology security policy, specifically the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). As part of implementing policy and meeting information assurance and privacy requirements, the US-VISIT Program maintains an audit function that tracks all user activities related to data including access and modification. These procedures and access logs are subject to management oversight that confirms compliance with privacy and security requirements. US-VISIT also seeks to prevent unauthorized access to data stored in its supporting systems through technical controls including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and ISAs that document controls for external connections, among other security methods. Periodically, US-VISIT, and the systems on which its information resides, is evaluated to ensure that it complies with the mandated privacy and security requirements.

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?

Given that carriers are collecting PII for US-VISIT processing, there is a risk that the carriers may misuse the PII or gain unauthorized access to DHS systems. There is also a risk that unauthorized individuals may gain access to the PII when it is transmitted from the carrier to DHS.

US-VISIT will seek to mitigate the risk of carriers misusing PII by establishing technical, security and privacy requirements for the carrier systems in standards guidance for carrier systems to be issued by DHS in conjunction with the Final Rule. Accordingly, US–VISIT is considering, and soliciting comment in the NPRM, the use of encryption upon collection to secure the biometrics against unauthorized use, disclosure, and modification while the biometrics reside on

carrier systems. Without clear restrictions on carrier use and retention of biometrics, the risk of misuse of biometrics by the carrier is high. It is DHS' expectation that the carriers will follow the requirements listed in the standards guide. However, to mitigate the risk effectively, an audit capability to ensure compliance with the restrictions may be necessary. A PIA will accompany the Final Rule and will assess the degree to which the requirements in the standards guidance for carrier systems are able to reduce the privacy risks associated with the Exit Program.

Furthermore, US-VISIT seeks to protect the integrity of the PII by requiring carriers to notify the US-VISIT Privacy Officer if a carrier experiences a security breach that may affect US-VISIT data. US-VISIT is also considering, and seeking comment in the NPRM, whether to mandate that carriers encrypt the biometrics upon collection. Encryption upon collection of biometrics would decrease the vulnerability of biometrics to unauthorized access, use or modification on the carriers' system from a moderate to low risk by taking the biometrics out of clear format when residing on carrier systems.

Additionally, US-VISIT mitigates the risk that carriers may gain unauthorized access to DHS systems by relying on indirect communication between the carrier system and the systems that directly support US-VISIT. Once the PII is received by DHS, existing US-VISIT privacy and security controls protect the information. The systems supporting US-VISIT are certified and accredited, and operated in accordance with US-VISIT and DHS policy and all applicable privacy and security regulations. These systems undergo a periodic assessment of physical, technical and administrative controls to enhance accountability and data integrity. Obtaining access to the systems is controlled through documented procedures based on least privilege, need to know, and established job responsibilities. These procedures and access logs are subject to management oversight that confirms compliance with privacy and security requirements. All individuals with access to the systems receive mandatory security and privacy training relevant to their role. Contractors and consultants must also sign a non-disclosure agreement. Detailed rules of behavior have also been developed to support the users acting within the systems.

US-VISIT mitigates the risk that unauthorized individuals obtain access to the PII in transmission by using an encrypted network between the carrier industry and DHS that complies with standards set forth in the ISAs required to be executed prior to external access to DHS systems.

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 What type of project is the program or system?

US-VISIT Exit is an operational project that establishes biometric exit verification capability. As proposed, US-VISIT Exit will rely on a combination of carrier systems to collect and transmit the PII to DHS, and government systems already supporting US-VISIT. These government systems, IDENT, ADIS, and APIS, are comprised of standard commercial technology and customized hardware and software required to meet the needs of DHS.

9.2 What stage of development is the system in and what project development lifecycle was used?

As proposed, US-VISIT Exit will rely on existing government systems supporting US-VISIT, a connection between the government and carrier systems, and a carrier system to collect the PII. US-VISIT systems, IDENT and ADIS, are operated and maintained in accordance with the Enterprise Life Cycle Methodology (ELCM). ELCM enables projects to follow a structured and repeatable process, from initial concept through to discrete business outcomes, which contributes to the overall success of the US-VISIT Program. APIS, a system owned by CBP, is operated and maintained on a CBP-approved System Development Lifecycle (SDLC). The interface and connection between the systems supporting US-VISIT and the carriers currently under development follows the US-VISIT ELCM process and is currently in the design phase. During the comment period of the proposed rule, US-VISIT will work with the carriers to develop the design and interface specifications necessary to support the carriers' transmission of the PII.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

As proposed, US-VISIT Exit relies on the same primary technologies that currently support the US-VISIT Program. The technologies consist of standard electronic communications and data storage systems. The matching algorithms used by US-VISIT to biometrically verify departure and conduct a biometric check against a list of subjects of interest do not present specific privacy concerns and are developed in an environment subject to strict administrative, technical and policy controls.

Given the sensitivity of the data and the need for a high degree of data integrity to ensure correct conclusions, US-VISIT has established an ELCM that embeds privacy risk assessment and documentation into project development. Technical and programmatic design choices are informed by this approach, such that proposed changes in terms of 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 principle are assessed. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

Approval Signature

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security