Privacy Impact Assessment Update
for the

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

In conjunction with the Final Rule (73 FR 77473), Enrollment of Additional Aliens in US-VISIT

February 10, 2009

Contact Point
Paul Hasson, Acting Privacy Officer
US-VISIT
(202) 298-5200

Reviewing Official
John W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is an integrated, automated biometric entry-exit system that records the arrival and departure of aliens; conducts certain terrorist, criminal, and immigration violation checks on aliens; and compares biometric identifiers to those collected on previous encounters to verify identity. US-VISIT is publishing this Privacy Impact Assessment (PIA) update in connection with the publication of the final rule to expand US-VISIT biometric collection requirements to cover additional classes of aliens. Under the final rule, effective January 18, 2009, 2008, US-VISIT will have the authority to process all aliens not explicitly exempted, with the exception of those Canadian citizens applying for admission as B-1/B-2 visitors for business or pleasure.[1]

Introduction

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is an integrated, automated biometric entry-exit system that records the arrival and departure of aliens; conducts certain terrorist, criminal, and immigration violation checks on aliens; and compares biometric identifiers to those collected on previous encounters to verify identity. US-VISIT has been implemented in stages, with each stage adding additional capabilities, locations of implementation, or populations. For each stage, US-VISIT has published a Privacy Impact Assessment (PIA), or an update that describes changes to the program from previous PIAs.

This PIA updates the US-VISIT PIA that analyzed the expansion of US-VISIT to cover additional categories of aliens, which was published on July 12, 2006, in support of a Notice of Proposed Rulemaking (NPRM) on the Authority to Process Additional Aliens in US-VISIT.[2] That PIA describes changes to the US-VISIT Program to extend US-VISIT biometric collection requirements to any alien (subject to specific exemptions as described below), with the exception of those Canadian citizens applying for admission as B-1/B-2 visitors for business or pleasure. The expansion to cover additional categories of aliens will be implemented with the addition of one or more additional categories of aliens as technological and operational resources permit. US-VISIT is publishing this PIA update to accompany the Final Rule on the Authority to Process Additional Aliens in US-VISIT. The final rule does not differ from the NPRM in any manner that would affect privacy; therefore, US-VISIT identified no additional privacy risks.

---

[1] On January 16, 2009 US-VISIT published technical revisions to the original rule published in December. The revisions did not affect the substance of the rule. The revisions can be found at 74 FR 2837.

[2] All US-VISIT PIAs are available for review on the DHS Privacy Office Web site – http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#13. The US-VISIT PIA Update, dated July 12, 2006, which specifically identifies the inclusion of additional aliens into the program, can be found at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addaliens.pdf.

Privacy Impact Analysis

On July 12, 2006, the Department of Homeland Security (DHS) published a PIA update in support of the NPRM published on July 27, 2006. The NPRM and PIA were published to modify US-VISIT regulations to provide that any alien may be processed through US-VISIT (subject to specific exemptions[3]), with the exception of those Canadian citizens applying for admission as B-1/B-2 visitors for business or pleasure.[4] Several large classes of aliens will be affected by this change including:

- U.S. Lawful Permanent Residents (LPRs)
- Aliens seeking admission on immigrant visas
- Refugees and asylees
- Certain Canadian citizens who receive a Form I-94 at inspection or who require waivers of inadmissibility
- Aliens paroled into the United States
- Aliens applying for admission under the Guam Visa Waiver Program

DHS received 69 comments in response to the July 27, 2006, NPRM. Twelve of these raised privacy issues. With regard to privacy, the comments received highlighted concerns in four areas: "mission creep," or concern that US-VISIT was expanding beyond its original purpose in a way that individuals who had participated in US-VISIT were not made aware of the full scope of the program; lack of right of judicial review for individuals affected by US-VISIT; privacy during the inspection process; and false hits, which occur on individuals incorrectly identified as subjects of interest.

Of the four areas of concern, the majority of comments focused on mission creep. That is, there was concern as to whether the US-VISIT Program was expanding beyond its scope as articulated in previous privacy and regulatory publications. As noted above, the US-VISIT Program has been implemented in stages, with each stage adding additional locations, capabilities, or covered populations. However, it has always been the case—and it is the statutory mandate—that US-VISIT cover all aliens entering and exiting the United States. The initial language described the US-VISIT-covered population as visitors or travelers, which may not have been previously viewed as including such groups of aliens as LPRs. Nevertheless, all of the authorizing statutes refer to "aliens" without differentiation. In addition, mission creep concerns were raised around the issue of using the information for law enforcement purposes. However, it is clear in the statutory language authorizing US-VISIT, as well as the regulatory and privacy publications, that US-VISIT

[3] The following categories of aliens are expressly exempt by regulation from US-VISIT biometric collection requirements: aliens admitted on A-1, A-2, C-3, G-1, G-2, G-3, G-4, NATO-1, NATO-3, NATO-4, NATO-5, or NATO-6 visas; children under the age of 14; persons over the age of 79; and certain officials of the Taipei Economic and Cultural Representative Office and members of their immediate families seeking admission on E-1 visas.

[4] 71 FR 42605

has national security and immigration law enforcement purposes, inasmuch as it coordinates with other DHS components that have specific law enforcement authority, such as U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE).

The second privacy concern was that DHS should offer a right of judicial review for individuals adversely affected by US-VISIT. DHS and the Department of Justice have consistently maintained that a determination of inadmissibility is excluded from judicial review and reviewable only pursuant to other statutory and regulatory provisions. See, e.g., section 240 of the Immigration and Naturalization Act (8 U.S.C. 1229a). However, if an individual believes that there is an error in the information contained in a DHS system that was collected through the US-VISIT process, DHS has provided a redress process to have records reviewed and amended or corrected based on accuracy, relevancy, timeliness, or completeness. This process includes confirming that mismatches and other errors are not retained as part of an alien's record. The first opportunity for data correction occurs at the port of entry, where CBP officers have the ability to manually correct most biographic errors, such as name, date of birth, flight information, and document errors.

There may be cases where individuals are no longer at the port of entry but believe that their data may be incorrect. For these situations, DHS has developed and implemented a centralized and well-publicized redress process, the Traveler Redress Inquiry Program (TRIP), which is described in detail online at www.dhs.gov/trip. TRIP provides persons with a fast and easy way to review personal information collected about them; to have information corrected as appropriate; and, if desired, to appeal redress decisions to the DHS Chief Privacy Officer. While millions of people have interacted with US-VISIT identity management services, US-VISIT has received only 437 petitions for redress out of more than 95 million encounters. Furthermore, the vast majority of these have largely centered on requests for information about the program, or were attempts to correct information to ensure that persons were not routinely selected for secondary inspection.

The third privacy issue was that, to enhance a covered individual's privacy, anyone sent to secondary inspection for purposes related to US-VISIT should be placed in a line separate and apart from those sent to secondary for other purposes. However, at the time that an individual is sent to secondary, the CBP officer does not know definitively whether the reason is related to US-VISIT or some other factor. Initial studies have determined, however, that the incidence of travelers being identified incorrectly as "watchlist hits" by US-VISIT and being referred to secondary as a result is low. At the time of publication and during the public comment period, this occurred less than one-tenth of 1 percent of the time anyone was sent to secondary.

The final privacy issue was that US-VISIT needs to be modified to reduce the impact of false hits—individuals who are incorrectly identified as watchlist hits. DHS is actively attempting

to decrease the likelihood of false hits with frequent upgrades of matching algorithms, technologies, and processes.

Risks Identified in Previous PIA

Data Collection

DHS is not collecting additional types of data from the US-VISIT-covered population; the covered population itself is growing. US-VISIT systems will face new performance and operational challenges because of the expanding covered population. However, this is a quantitative rather than qualitative change to an existing privacy risk. DHS mitigates the privacy risk of this expansion by expanding biometric-matching system capabilities with extensive security measures to protect US-VISIT systems; and through additional system education and training, policies, and procedures provided to users in handling this data.

Data Use

There are no new uses of data based on the changes to US-VISIT necessitating this PIA. However, there is a potential privacy risk because an incorrect decision may be made based on potentially inaccurate data from the transfer of historical U.S. Citizenship and Immigration Services (USCIS) data in the DHS Automated Biometric Identification System (IDENT). To mitigate such a risk, US-VISIT uses a quality assurance process to identify any errors in properly matching individuals with relevant records (e.g., special checks targeted at specific data elements exhibiting a statistically significant tendency to cause matching errors).

Data Disclosure

Nevertheless, 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 sharing organizations to develop secure standard operating procedures for sharing this data. These procedures are documented in sharing agreements. In all cases of sharing internal to DHS, all organization are required to comply with the Department's security policies and procedures.

Conclusion

Considering all of the comments DHS received, and specifically the comments received with regard to privacy issues, DHS is adopting the proposed rule of July 27, 2006, as the final rule and so will include the additional categories of aliens, as described above, as US-VISIT-covered persons.

Responsible Official

Paul Hasson, Acting Privacy Officer
US-VISIT
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

John W. Kropf
Acting Chief Privacy Officer
Department of Homeland Security