

## **Human Rights First Concerns about US-VISIT's Implications on Asylum Seekers' Confidentiality and Safety\***

### Background on Asylum Seekers

As defined by the 1951 Refugee Convention and 1967 Protocol relating to the Status of Refugees, a refugee is any person who fears persecution “for reasons of race, religion, nationality, membership of a particular social group, or political opinion.”<sup>1</sup> The United States enacted the Refugee Act in 1980<sup>2</sup>, which brought the United States into conformance with the Convention.<sup>3</sup> The United States offers protection to refugees through its asylum system. Asylum seekers apply for asylum in the United States through a rigorous screening procedure which vets applicants for fraud, insufficient grounds for asylum, and security concerns.

Asylum-seekers are different than other nonimmigrant visa holders arriving in the United States because of the reasons that forced them to leave their home country. Due to fear of persecution, asylum-seekers often leave without the opportunity to complete the required visa process for travel. Consequently, they may travel with false documentation or without any documentation at all. They also may be emotionally and physically unprepared for the rigors of travel and may be reluctant to trust any government officials because of their past negative experiences. Often, they have been forced to leave behind family members and friends whose safety may still be in question. Accordingly, asylum-seekers are extremely wary of sharing sensitive information and face extraordinary risk should such their privacy be compromised.

### Background on US-VISIT

US-VISIT, the United States Visitor and Immigrant Status Indiciary Technology, is a Department of Homeland Security (DHS) program designed to monitor nonimmigrant visa-holders in the United States in order to enhance national security. US-VISIT integrates existing security and monitoring measures that begin before an individual enters the United States and continue through arrival and departure from the United States.

---

\* This memo was written by Glenna MacGregor, a second year law student at Georgetown University Law Center, and legal intern at Human Rights First.

<sup>1</sup> United Nations Convention relating to the Status of Refugees, *opened for signature* July 28, 1951, 19 U.S.T. 6259, 189 U.N.T.S. 137; United Nations Protocol relating to the Status of Refugees, *opened for signature* Jan. 31, 1967, 19 U.S.T. 6223, 606 U.N.T.S. 267 [together hereinafter U.N. Convention].

<sup>2</sup> Refugee Act of 1980, Pub. L. No. 96-212, 94 Stat. 102 (1980) (codified as amended in scattered sections of 8 U.S.C.)

<sup>3</sup> *See* INS v. Cardoza-Fonseca, 480 U.S. 421, 436-37 (1987).

US-VISIT emerged in response to two mandates from Congress<sup>4</sup> to the Attorney General to develop and integrate automated entry and exit monitoring systems for every foreign visitor entering and departing from the United States. US-VISIT was significantly expanded by the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), passed by Congress in response to the terrorist acts of September 11, 2001.<sup>5</sup> The Act imposed a timeline for the program's implementation and introduced the possible use of biometrics for establishing a technological standard for US-VISIT. US-VISIT was further augmented by the Enhanced Border Security and Visa Entry Reform Act of 2002, which increased the integration of US-VISIT with other law enforcement and intelligence monitoring and record-keeping systems and mandated accessibility of the systems to officials responsible for "the investigation or identification of aliens."<sup>6</sup>

DHS intends to use the information collected under US-VISIT for "national security, law enforcement, and immigration control," in addition to "other functions." This last category includes collection of intelligence, immigration investigations, prosecution or law enforcement.

Increment 1 of US-VISIT, which was implemented on December 31, 2003, consists of the collection and verification of biometric information of foreign nationals arriving with nonimmigrant visas at air and seaports of entry. Increment 1 integrates the capabilities of three existing systems<sup>7</sup> and incorporates pre-arrival eligibility determinations made by both the DHS and the Department of State.

#### Security of Information Compiled by US-VISIT

The information collected by US-VISIT is accessible by officials from the Customs Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Citizenship and Immigration Services (CIS), as well as the Transportation Security Administration (TSA). According to the US-VISIT Privacy Impact Assessment (PIA), information may be shared with other law-enforcement agencies who are "lawfully engaged in collecting law enforcement intelligence information and who need access to the information in order to carry out their law enforcement duties." Other agencies mentioned include foreign law-enforcement agencies.

---

<sup>4</sup> Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. 104-208, Div. C, Title III, § 309 (1996), *amended by* the Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. 106-215, 114 Stat. 337 (2000).

<sup>5</sup> Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

<sup>6</sup> Enhanced Border Security Act and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat. 543 (2002).

<sup>7</sup> The Arrival and Departure System (ADIS); the Passenger Processing Component of the Treasury Enforcement Communications System (TECS); and the Automated Biometric Identification System (IDENT).

Existing DHS security guidelines provide protection of the information collected by US-VISIT. The PIA describes “multi-layer mechanisms that are physical, technical, administrative and environmental,” including access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication process of sending parties, and screening of personnel with access. The privacy controls foreseen by DHS include:

- Privacy sensitivity awareness programs for US-VISIT operators;
- Establishment of a US-VISIT privacy officer and accountability program for those responsible for compliance with the US-VISIT Privacy Policy;
- Periodic reviews of collected data;
- Usage agreements between US-VISIT and other agencies who have access to the program;
- Creation of limited opportunities for covered individuals to have access to their information and/or to allow them to challenge its completeness;
- Maintenance of security safeguards to prevent unauthorized disclosure; and
- Establishment of administrative controls to prevent improper actions due to data inconsistencies from multiple information sources.

While we are encouraged by DHS’s attention to the general privacy concerns of the US-VISIT program and the security problems they implicate, for the reasons cited below we remain apprehensive that the privacy measures envisioned will not be adequate to account for the unique security concerns of asylum-seekers entering the United States.

#### Confidentiality Concerns of Asylum-Seekers

Asylum-seekers arrive in the United States after fleeing persecution in another country. They have often fled out of desperation, possibly leaving behind friends and family members who at the very least know of the circumstances that led to persecution, if not risk persecution themselves. If the government of an asylum-seeker were to be made knowledgeable of the presence and intentions of the asylum-seeker in the United States, the government could use the information in a retaliatory manner to threaten or to persecute those friends and family members that remain in the country.

Another danger of disclosure to foreign governments emerges in the event that a failed asylum-seeker returns to his/her country of origin and risks personal retaliation by the government. A government may target a failed asylum-seeker for basic purposes of retribution or to make an example of the consequences of fleeing the country and seeking asylum elsewhere. The simple fact that an asylum-seeker even applied for asylum may make him/her vulnerable, regardless of the content or basis for the asylum application.

These concerns may be even more significant for asylum-seekers in the Immigration Court stage as compared to affirmative asylum cases.<sup>8</sup> In the former, immigration officials more aggressively pursue forensic testing of identity and other evidentiary documentation. In some cases, those efforts have included sharing information with government officials in the countries of past or feared prosecution.

Concerns regarding the confidentiality of information related to asylum applications existed prior to the legislation drafted in the wake of the terrorist attacks on September 11, 2001.<sup>9</sup> Although federal regulation required INS not to disclose information pertaining to or revealing the existence of an asylum application without written consent of the asylum-seeker, disclosure without that consent was permitted at “the discretion of the Attorney General.” That exception for exercise of the Attorney General’s discretion has been preserved in the transition from INS to DHS.<sup>10</sup>

Certain measures have been taken at both legislative and policy levels to account for these asylum-related confidentiality concerns. Regulations governing DHS mandate that records indicating that a specific alien has applied for asylum be “protected from disclosure.” DHS is required to coordinate with the Department of State to ensure that the confidentiality of those records is maintained if they are shared with Department of State offices abroad.<sup>11</sup>

On Department of State web pages outlining the basic requirements of consular notification, the guidelines indicate that precautions can be taken when there is a possibility that a foreign national has a legitimate fear of persecution or other mistreatment by his/her government. The instructions regarding consular notification in asylum cases are even clearer: “*under no circumstances should any information indicating that a foreign national may have applied for asylum in the United States or elsewhere be disclosed to that person's government*” (italics in original).<sup>12</sup> These comments by the Department of State suggest an awareness of the unique danger of confidentiality breaches facing an asylum-seeker. The policy has also been implemented in DHS regulations regarding consular notifications.<sup>13</sup>

---

<sup>8</sup> An asylum seeker can apply for asylum in two different manners. 8 C.F.R. § 208.14. If an asylum seeker is admitted (through a visa or otherwise) into the United States, the person can file an application with Bureau of Citizenship and Immigration Services (part of DHS) within one year of arrival requesting asylum. An asylum officer will then interview the applicant and may grant asylum. The officer may also refer the case to an immigration judge if the officer is not convinced that applicant is eligible for relief and in limited instances the officer may deny asylum. The immigration judge will review the asylum claim de novo. If a person is stopped at the border and requests asylum that person will not be afforded the opportunity to apply affirmatively, instead the immigration judge will be the first official to review the applicant’s claim for asylum.

<sup>9</sup> Beth Lyon, *Fighting a Deadling on Fear: Asylum Practice Update as the One-Year Deadline Approaches*, 75 No. 8 Inter. Rel. 285 (1998).

<sup>10</sup> 8 C.F.R. § 208.6.

<sup>11</sup> Id.

<sup>12</sup> <<http://travel.state.gov/notification2.html>> (last visited Apr. 9, 2004).

<sup>13</sup> 8 CFR § 236.1(e): (“When notifying consular or diplomatic officials, Service officers shall not reveal the fact that any detained alien has applied for asylum or withholding of removal.”)

Despite the policy and legislative references to confidentiality concerns specific to asylum-seekers, US-VISIT remains unequipped to sufficiently address the risks of information-sharing with foreign governments. The DHS regulations governing disclosure still grant broad discretion to the Attorney General. The climate of post-September 11 immigration control has been characterized by extensive exercise of the Attorney General's discretionary powers. Attorney General Ashcroft has stated publicly that he will use the full extent of immigration law as an enforcement mechanism against terrorism.<sup>14</sup> There is no guarantee that his pursuit of terror suspects will leave existing protections for asylum-seekers undisturbed.

Until specific accounting for confidentiality concerns of asylum seekers is incorporated into US-VISIT, asylum-seekers arriving in the United States risk retaliation from their governments.

### Recommendations

We are encouraged by DHS's openness to comments on the privacy implications of US-VISIT. Accordingly, we have developed recommendations that would enable DHS to address the confidentiality concerns of asylum-seekers:

- Though admission to the US is contingent upon cooperation with US-VISIT requirements, a discretionary waiver under the Immigration Nationality Act may be granted. DHS could provide for a waiver specific to sensitive information regarding asylum applications.
- Privacy concerns specifically facing asylum-seekers could be included in the "sensitivity-awareness training" given to US-VISIT personnel.
- Guidelines in the usage agreements between US-VISIT and other agencies could include non-disclosure requirements for information regarding asylum applications. DHS could look to United Nations High Commissioner for Refugees (UNHCR) policy for guidance on information sharing with foreign governments about asylum applicants.
- Any individual granted any relief – asylum, withholding of removal, etc. – has already been thoroughly reviewed for terrorist connections or other security concerns. These individuals could have information removed from the US-VISIT database or otherwise made unavailable.
- DHS should seek further advice from UNHCR on this issue, through the establishment of regular meetings convened on this topic.
- Recent reports indicate that there will be internal audits on privacy concerns related to US VISIT. These audits could include investigation relevant to the special needs of asylum-seekers.
- The PIA indicates that "Memoranda of Understanding and of Agreement are being negotiated with third parties (including other agencies) that will address protection and use of US-VISIT data to mitigate the risk that the information collected is being

---

<sup>14</sup> Attorney General John Ashcroft Outlines Foreign Terrorist Tracking Task Force (Oct. 31, 2001), <[http://www.usdoj.gov/ag/speeches/2001/agcrisisremarks10\\_31.htm](http://www.usdoj.gov/ag/speeches/2001/agcrisisremarks10_31.htm)> (last visited Apr. 16, 2004).

used for purposes other than the legitimate goals of US VISIT.” These Memoranda could address the confidentiality concerns of asylum-seekers.