

DEPARTMENT OF HOMELAND SECURITY

Bureau of Immigration and Customs Enforcement  
Bureau of Customs and Border Protection

Docket. No. DHS/ICE-CBP-001  
Notice of Privacy Act System of Records

---

**COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER**

By notice published on December 12, 2003, the Department of Homeland Security (“DHS”) announced that the previously established Arrival Departure Information System (“ADIS”) will collect biometric and biographic data for use by the United States Visitor and Immigrant Status Technology (“US-VISIT”).<sup>1</sup> Pursuant to the DHS notice, the Electronic Privacy Information Center (“EPIC”) submits these comments to ask that DHS not exempt ADIS from any Privacy Act requirements, to urge the agency to reduce its 100-year data retention proposal, and to consider the significance of international privacy standards in the collection and use of personal information by U.S. agencies on non-U.S. citizens.

Arrival Departure Information System (“ADIS”)

ADIS is one of approximately twenty existing information systems that has become a component system of US-VISIT, a program intended to allow the government to collect information about foreign nationals traveling to the United States.<sup>2</sup> According to the notice, “ADIS is a system of records tracking immigrants, nonimmigrants and

---

<sup>1</sup> Notice of Privacy Act System of Records, 68 Fed. Reg. 69412 (Dec. 12, 2003).

<sup>2</sup> General Accounting Office, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to be Addressed* at 32 (Sept. 2003).

Lawful Permanent Residents arriving in and departing from the United States. It enables the Secretary of Homeland Security to identify, through on-line searching procedures, lawfully admitted nonimmigrants who remain in the United States beyond the period of authorized stay, and to analyze information gathered for the purpose of this and other DHS programs.”<sup>3</sup> ADIS includes numerous data elements, including “arrival and departure information, . . . complete name, date of birth, nationality, gender, passport number and country of issuance, country of residence, U.S. visa number including date and place of issuance if applicable, alien registration number if applicable, immigration status, complete address while in the United States, and Fingerprint Identification System (FINS) number.”<sup>4</sup> The notice acknowledges that that in addition to containing information on foreign nationals subject to US-VISIT, ADIS “contains biographic arrival/departure information on *legal permanent residents*.”<sup>5</sup> (Emphasis added).

ADIS Should Not Be Exempt From Privacy Act Requirements Merely Because the System is Part of US-VISIT

The Privacy Act applies to an agency’s creation and maintenance of a “system of records,” which is defined as a group of records under the control of an agency “from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”<sup>6</sup> A “record” is any item or collection of information about an individual which is maintained by an

---

<sup>3</sup> 68 Fed. Reg. at 69413.

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> 5 U.S.C. § 552a(a)(5).

agency and which contains that individual's name or other identifying particular.<sup>7</sup> Significantly, the Act defines an "individual" as "a citizen of the United States or an alien lawfully admitted for permanent residence."<sup>8</sup> Neither United States citizens nor aliens lawfully admitted for permanent residence are subject to information collection via US-VISIT.<sup>9</sup>

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."<sup>10</sup> It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.<sup>11</sup>

DHS's Chief Privacy Officer recently touted the protections afforded by the Privacy Act (and the purpose of a notice like the one at issue here), explaining that the law:

provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, though detailed 'system of records' notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.<sup>12</sup>

---

<sup>7</sup> 5 U.S.C. § 552a(a)(4); *see also White v. Civil Service Comm'n*, 589 F.2d 713 (D.C. Cir. 1978).

<sup>8</sup> 5 U.S.C. § 552a(a)(2).

<sup>9</sup> 69 Fed. Reg. at 471.

<sup>10</sup> Pub. L. No. 93-579 (1974).

<sup>11</sup> *Id.*

<sup>12</sup> Remarks of Nuala O'Connor Kelly Before the 25th International Conference of Data Protection and Privacy Commissioners, Sydney, Australia, Sept. 11, 2003.

The notice published by DHS, however, exempts ADIS from nearly all of the Privacy Act provisions Ms. O'Connor Kelly described.

The notice announces that ADIS will be exempt from eleven provisions of the Privacy Act to the full extent possible under law.<sup>13</sup> Among the obligations DHS has exempted the ADIS system of records from are:

- DHS's duty to give an individual, at his request, an accounting of disclosures to others.<sup>14</sup>
- DHS's duty to inform other agencies of corrections to or disputes about the content of a record.<sup>15</sup>
- DHS's duty to allow an individual to review his records and have copies made.<sup>16</sup>
- DHS's duty to permit an individual to ask that a record be amended, as well as appeal an agency's refusal to amend a record.<sup>17</sup>
- DHS's duty to correct information that an individual believes is not accurate, timely, relevant or complete.<sup>18</sup>
- DHS's duty to maintain only information that is relevant and necessary to carry out a task required of the agency by law.<sup>19</sup>
- An individual's right to enforce his rights judicially under the Privacy Act.<sup>20</sup>

---

<sup>13</sup> 68 Fed. Reg. 69414.

<sup>14</sup> 5 U.S.C. § 552a(c)(3).

<sup>15</sup> 5 U.S.C. § 552a(c)(4).

<sup>16</sup> 5 U.S.C. § 552a(d)(1).

<sup>17</sup> 5 U.S.C. § 552a(d)(2), (d)(3).

<sup>18</sup> 5 U.S.C. § 552a(d)(2)(B)(i).

<sup>19</sup> 5 U.S.C. § 552a(e).

<sup>20</sup> 5 U.S.C. § 552(a)(g).

DHS should not use US-VISIT as a justification for exempting ADIS from Privacy Act requirements. The reason given for publishing this Privacy Act notice is to “allow[ ] the ADIS system to collect biometric and biographic data for US-VISIT.”<sup>21</sup> However, the Privacy Act protects only records of “a citizen of the United States or an alien lawfully admitted for permanent residence[.]”<sup>22</sup> Yet, according to DHS, the US-VISIT program currently collects and contains information only about “aliens applying for admission pursuant to a nonimmigrant visa who arrive in or depart from the United States through designated air and sea ports.”<sup>23</sup> If that is the case, US-VISIT should not involve the collection or use of records of any persons entitled to protection under the Privacy Act.<sup>24</sup>

It is not clear why DHS cites the use of ADIS within US-VISIT to exempt the system from Privacy Act requirements. If the ADIS system does not affect individuals protected by the Privacy Act, EPIC asks that DHS not exempt ADIS from any Privacy Act requirements without a stronger justification for doing so. However, if DHS does expect that the system’s use within US-VISIT may affect individuals protected by the Privacy Act, EPIC asks that the agency make clear why it sees fit to exempt this system from Privacy Act requirements.

---

<sup>21</sup> 68 Fed. Reg. at 69412.

<sup>22</sup> 5 U.S.C. § 552a (a)(2).

<sup>23</sup> 69 Fed. Reg. at 471.

<sup>24</sup> If individuals protected by the Privacy Act are afforded so few rights in information maintained in ADIS, it will be interesting to see what access and redress procedures DHS provides for foreign nationals who are actually subject to US-VISIT and may be negatively impacted if the program is inefficient or produce erroneous results.

### A 100 Year Data Retention Period is Unnecessary to Accomplish US-VISIT's Goals

The notice further provides that “records [in ADIS] will be retained for 100 years.”<sup>25</sup> This period of time far exceeds a record’s period of usefulness and will contribute to a problem already identified by DHS. The Privacy Impact Assessment recently released by DHS noted that inconsistencies within and duplication of information maintained in the US-VISIT component systems “result in some heightened degree of risk with respect to integrity/security of data . . . because personal information could persist on one or more component systems beyond its *period of use* or disappear from one or more component systems while still in use.”<sup>26</sup> To maintain records in ADIS for 100 years clearly exceeds the information’s useful life for US-VISIT purposes, and is an unnecessary invasion of privacy. Therefore, DHS should reduce the period of time for which it will retain records in ADIS.

### As it Implements US-VISIT, DHS Should Consider International Standards Governing the Collection and Use of Personal Information on Non-U.S. Citizens

Though no U.S. law currently requires DHS to protect the privacy of non-U.S. citizens as the agency develops and deploys US-VISIT, EPIC urges DHS to consider the application of international privacy standards to the collection and use of personal information obtained for non-U.S. citizens. The international community has recognized time and time again that all individuals have rights in their personal information, regardless of nationality.

---

<sup>25</sup> 68 Fed. Reg. at 69414.

<sup>26</sup> Department of Homeland Security, *US-VISIT Program, Increment 1 Privacy Impact Assessment* (Dec. 18, 2003) at 7.

The Universal Declaration of Human Rights (“Universal Declaration”) provides that no individual “shall be subjected to arbitrary interference with his privacy,” and that “[e]veryone has the right to protection of the law against such interference or attacks.”<sup>27</sup> Furthermore, “no distinction shall be made on the basis of the political, jurisdictional, or *international* status of the country or territory to which a person belongs[.]”<sup>28</sup> (Emphasis added.) The United States was a key architect of the Universal Declaration and one of the original signatories. However, the US-VISIT program violates the Universal Declaration by encroaching upon the privacy of individuals based on their lack of U.S. citizenship, and fails to provide them rights in their personal information held by the United States.

The OECD Privacy Guidelines of 1980 (“OECD Guidelines”) apply to “personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.”<sup>29</sup> The OECD Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information’s existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as

---

<sup>27</sup> United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in M. ROTENBERG ED., THE PRIVACY LAW SOURCEBOOK 2003 318 (EPIC 2003) [hereinafter PRIVACY LAW SOURCEBOOK].

<sup>28</sup> *Id.*, art. 2. at 318.

<sup>29</sup> Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc. 58 final (Sept. 23, 1980), art. 3(a), reprinted in PRIVACY LAW SOURCEBOOK at 330.

appropriate.<sup>30</sup> US-VISIT will deny non-U.S. citizens the fundamental protections of these internationally recognized standards.

The United Nations Guidelines for the Regulation of Computerized Personal Files of 1990 (“UN Guidelines”) recognize many of the same rights in information as the OECD Guidelines provide, stating in addition that “data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, philosophical and other beliefs . . . should not be compiled.”<sup>31</sup> The US-VISIT program may collect and use information of this nature to evaluate whether visitors may enter the United States, which clearly violates the UN Guidelines.

In addition, the European Union Data Protection Directive (“EU Directive”) recognizes a right to privacy in personal information and establishes protections for information collected from all individuals, regardless of nationality.<sup>32</sup> Like both sets of Guidelines, the EU Directive recognizes an individual’s right to access information and requires that information be kept accurate and timely.<sup>33</sup> The EU Directive also requires that information be relevant to the purpose for which it is collected.<sup>34</sup> By neglecting to give non-U.S. citizens rights in information about them used in the US-VISIT program,

---

<sup>30</sup> *Id.*, Basic Principles of National Application at 331.

<sup>31</sup> United Nations, G.A. Res. 45/95, Guidelines for the Regulation of Computerized Personal Files (Dec. 14, 1999) prin. 5, reprinted in PRIVACY LAW SOURCEBOOK at 368.

<sup>32</sup> Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, reprinted in PRIVACY LAW SOURCEBOOK at 371.

<sup>33</sup> *Id.*, art. 6 at 384.

<sup>34</sup> *Id.*

the United States has failed to comply with this widely recognized legal regime for privacy protection.

The United States is a signatory of the Universal Declaration, OECD Guidelines, and UN Guidelines, and is bound to follow their provisions. The United States's collection and use of personal information of non-U.S. citizens through the US-VISIT program violates these guidelines and the EU Directive, and shows disregard for international privacy laws and human rights standards.

### Conclusion

For the forgoing reasons, EPIC believes that DHS should not exempt ADIS from any Privacy Act requirements due to the system's integration into US-VISIT program, urges the agency to reduce its proposed 100-year data retention period, and suggests that DHS consider the application of international standards for collection and use of non-U.S. citizens' information as it further develops and deploys US-VISIT.

Respectfully submitted,

Marc Rotenberg  
Executive Director

David Sobel  
General Counsel

Marcia Hofmann  
Staff Counsel

ELECTRONIC PRIVACY INFORMATION CENTER  
1718 Connecticut Avenue, N.W., Suite 200  
Washington, DC 20009  
(202) 483-1140