9110-9P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2013-0039]

Privacy Act of 1974; Department of Homeland Security National Protection and Programs Directorate – 001 Arrival and Departure Information System, System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to update and reissue a Department of Homeland Security system of records titled Department of Homeland Security/National Protection and Programs Directorate – 001 Arrival and Departure Information System (ADIS) System of Records (72 FR 47057, August 22, 2007). This system of records allows the Department of Homeland Security to collect and maintain records on individuals throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes.

With the publication of this updated system of records, the following changes are being made: (1) a new category of records is being added; (2) the record source categories are being updated; and (3) administrative updates are being made globally to comply with the Consolidated and Further Continuing Appropriations Act of 2013, which transfers the United States Visitor Indicator Technology (US-VISIT) program's biometric identity management functions to the Office of Biometric Identity Management (OBIM),

a newly created office within DHS/National Protection and Programs Directorate (NPPD).

The exemptions for the existing system of records notice will continue to be applicable for this updated system of records notice and this system will be continue to be included in the Department of Homeland Security's inventory of record systems.

DATES AND COMMENTS: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This updated system will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. In particular, comments are requested concerning the application of the exemptions to the new category of records.

ADDRESSES: You may submit comments, identified by docket number DHS-2013-0039 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Emily Andrew, (202) 298-5200, Senior Privacy Officer, National Protection and Programs Directorate, Mailstop 0655, 245 Murray Lane, Washington, DC 20528. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Office of Biometric Identity Management (OBIM) proposes to update and reissue a current DHS system of records titled, "DHS/NPPD - 001 Arrival and Departure Information System (ADIS) System of Records" (72 FR 47057, August 22, 2007). A Final Rule exempting this system of records from certain provisions of the Privacy Act was published on August 22, 2007 (72 FR 46921).

ADIS is a system for the storage and use of biographic, biometric indicator, and encounter data on aliens who have applied for entry, entered, or departed the United States (U.S.). ADIS consolidates information from various systems in order to provide a repository of data held by DHS for pre-entry, entry, status management, and exit tracking of immigrants and non-immigrants. Its primary use is to facilitate the investigation of subjects of interest who may have violated their immigration status by remaining in the United States beyond their authorized stay. The information is collected by, on behalf of,

in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, tribal, foreign, or international government agencies.

This system of records notice updates the categories of records and record source categories. Originally, records could be derived from entry or exit data of foreign countries collected by foreign governments in support of their respective entry and exit processes. These records collected from foreign governments were required to relate to individuals who have an existing record in ADIS. This update clarifies that although records collected from foreign governments must relate to individuals who have entered or exited the United States, in some instances there may be no pre-existing ADIS record for those individuals.

In March 2013, the Consolidated and Further Continuing Appropriations Act of 2013 (The Act) transferred the legacy US-VISIT overstay analysis mission to DHS/Immigration and Customs Enforcement (ICE) and the entry/exit policy to DHS/Customs and Border Protection (CBP). The Act also transferred the program's biometric identity management functions to the Office of Biometric Identity Management (OBIM), a newly created office within NPPD. Administrative updates are being made globally to comply with these changes.

Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS' information-sharing mission, information stored in the DHS/NPPD - 001 Arrival and Departure Information System (ADIS) may be shared with

other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

The exemptions for the existing system of records notice will continue to be applicable for this updated system of records notice and this system will continue to be included in DHS' inventory of record systems. In the context of this updated system of records notice, the Department is requesting comment on the application of the exemptions to the newly added category of records.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/NPPD-001 Arrival and Departure

Information System (ADIS) System of Records.

In accordance with 5 U.S.C. § 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/National Protection and Programs Directorate (NPPD) – 001.

System name:

DHS/NPPD – 001 Arrival and Departure Information System (ADIS).

Security classification:

Unclassified.

System location:

Records are maintained at the DHS/NPPD Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:

Categories of individuals covered by this notice consist of aliens who have applied for entry, entered, or departed from the United States at any time. These individuals may be in records collected by DHS or other Federal, state, local, tribal, foreign, or international government organizations. This system primarily consists of records pertaining to alien immigrants (including lawful permanent residents) and non-immigrants. Some of these individuals may change status and become United States citizens.

Categories of records in the system:

ADIS contains biographic data, biometric indicator data, and encounter data. Biographic data includes, but is not limited to, name, date of birth, nationality, and other personal descriptive data. Biometric indicator data includes, but is not limited to, fingerprint identification numbers. Encounter data provides the context of the interaction between the immigrant or non-immigrant and the border management authority. This data includes, but is not limited to, encounter location, document types, document numbers, document issuance information, and address while in the United States.

ADIS also sometimes contains commentary from immigration enforcement officers, which includes references to active criminal and other immigration enforcement investigations and contains other confidential data fields used for enforcement purposes.

ADIS data may be derived from records related to entry or exit data of foreign countries collected by foreign governments in support of their respective entry and exit processes. Generally, records collected from foreign governments relate to individuals who have entered or exited the United States at some time, but in some instances there is no pre-existing ADIS record for the individual.

Authority for maintenance of the system:

6 U.S.C. § 202; 8 U.S.C. §§ 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, and 1732.

Purpose(s):

This system of records is the primary repository of data held by DHS for near real-time entry and exit status tracking throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes, based on data collected by DHS or

other federal or foreign government agencies and used in connection with DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. Data is also used to provide associated testing, training, management reporting, planning and analysis, or other administrative purposes. Similar data may be collected from multiple sources to verify or supplement existing data and to ensure a high degree of data accuracy.

Specifically, the ADIS data will be used to identify lawfully admitted non-immigrants who remain in the United States beyond their period of authorized stay, which may have a bearing on an individual's right or authority to remain in the country or to receive governmental benefits; to assist DHS in supporting immigration inspection at ports of entry (POE) by providing quick retrieval of biographic and biometric indicator data on individuals who may be inadmissible to the United States; and to facilitate the investigation process of individuals who may have violated their immigration status or may be subjects of interest for law enforcement or intelligence purposes.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

A. To 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 related to administering or enforcing the law, national security, or immigration, when consistent with a DHS mission-related function as determined by DHS.

B. To appropriate federal, state, local, tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of such an employee, the letting of a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency.

C. To an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, or discovery proceedings.

D. To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.

E. To the National Archives and Records Administration (NARA) or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish a DHS mission function related to this system of records in compliance with the Privacy Act of 1974.

G. To appropriate agencies, entities, and persons when: (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DHS has determined that, as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

H. To federal, state, local, tribal, foreign or international government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, digital media.

Retrievability:

Records may be retrieved by a variety of data elements including, but not limited to, name, place and date of arrival or departure, document number, and fingerprint identification number.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

The following proposal for retention and disposal is pending approval with the National Archives and Records Administration (NARA): Testing and training data will be purged when the data is no longer required. Electronic records for which the statute of limitations has expired for all criminal violations or that are older than 75 years, whichever is longer, will be purged.

System Manager and address:

ADIS System Manager, OBIM, U.S. Department of Homeland Security, Washington, DC 20528.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the

notification, access, and amendment procedures of the Privacy Act because it may contain records from a law enforcement system. However, DHS/NPPD will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the DHS/NPPD FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;

- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Basic information contained in this system is supplied by individuals covered by this system and other federal, state, local, tribal, or foreign governments; private citizens; and public and private organizations.

ADIS data may be derived from records related to entry or exit data of foreign countries collected by foreign governments in support of their respective entry and exit processes. Generally, records collected from foreign governments relate to individuals

who have entered or exited the United States at some time, but in some instances there is no pre-existing ADIS record for the individual.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted this system from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). In addition, the Secretary of Homeland Security has exempted portions of this system from 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f) pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. § 552a(j)(2) and (k)(2).

Dated: May 16, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-12390 Filed 05/24/2013 at 8:45 am; Publication Date: 05/28/2013]