9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0073]

Privacy Act of 1974; Department of Homeland Security/U.S. Customs and Border Protection-021 Arrival and Departure Information System

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 proposes to update, rename, and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/U.S. Customs and Border Protection-021 Arrival and Departure Information System." This system of records allows the Department of Homeland Security/U.S. Customs and Border Protection to collect and maintain records on individuals throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes.

The Department of Homeland Security/U.S. Customs and Border Protection is updating this system of records notice to make the following changes/updates: (1) addition of a new category of records; (2) updated routine uses; and (3) administrative updates to reflect the transfer of the entry-exit program from the Office of Biometric Identity Management, an office within Department of Homeland Security, National Protection and Programs Directorate, to the U.S. Customs and Border Protection in accordance with the Consolidated and Further Continuing Appropriations Act of 2013.

With the publication of this updated system of records, the Department of Homeland Security will retire the former version of the system of records titled, "Department of Homeland Security/National Protection and Programs Directorate--001 Arrival and Departure Information System of Records," and complete the transfer of the entry/exit program to U.S. Customs and Border Protection. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

The exemptions for the existing system of records, published in the Final Rule dated December 4, 2009 (74 FR 63944) 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: 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].

ADDRESSES: You may submit comments, identified by docket number DHS-2015-0073 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: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

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: John Connors, (202) 344-1610, Privacy Officer, U.S. Customs and Border Protection, Privacy and Diversity Office, 1300 Pennsylvania Ave, N.W. Washington, D.C. 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) proposes to update, rename, and reissue a DHS system of records titled, "DHS/CBP-021 Arrival and Departure Information System (ADIS) System of Records," previously published as "Department of Homeland Security National Protection and Programs Directorate-001 Arrival and Departure Information System, System of Records" (78 FR 31955, May 28, 2013). A Final Rule exempting this system of records from certain provisions of the Privacy Act was published on December 4, 2009 (78 FR 63943) and continues to be applicable.

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. 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. CBP uses ADIS to determine whether individuals have maintained legal status and to facilitate investigations of the status of individuals who remain 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 (PII) collected by other federal, state, local, tribal, foreign, or international government agencies.

DHS/CBP is making several updates as it republishes this system of records notice (SORN). First, CBP is adding a new category of records to the system of records. CBP is including Social Security numbers (SSN) as a new category of records, when they are available, to address SSNs that may be contained in immigration status adjustment or other U.S. Citizenship and Immigration Services (USCIS) records. CBP is also adding four new routine uses (A, D, G, and N) that address data sharing for litigation purposes, audits, investigations, and in certain limited instances when there exists a legitimate public interest in disclosing the information. CBP is also adding a new routine use (L) to provide transparency about CBP's sharing of ADIS information with other federal agencies for the purpose of determining proper payment of federal benefits to the subject of the record in accordance with that agency's statutory responsibilities. Finally CBP is making administrative updates to reflect the transfer of the entry/exit program from the legacy United States Visitor Indicator Technology (US-VISIT) to DHS/CBP as mandated

by the Consolidated and Further Continuing Appropriations Act of 2013. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information-sharing mission, information stored in 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 consistent with applicable exemptions under the Privacy Act, including routine uses set forth in this SORN that provide for sharing with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies.

The exemptions for the existing SORN will continue to be applicable for this updated SORN and this system will continue to be included in DHS's inventory of record systems. In addition to the new routine uses, new category of records, and other changes to this SORN, 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/CBP-021 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)/U.S. Customs and Border Protection (CBP)-021.

System name:

DHS/CBP-021 Arrival and Departure Information System (ADIS).

Security classification:

Unclassified.

System location:

CBP maintains ADIS data at DHS/CBP Headquarters in Washington, D.C., DHS/CBP data centers in Mississippi and Virginia, and in field offices that receive access to limited data.

Categories of individuals covered by the system:

Categories of individuals consist of aliens who have applied for entry, entered, or departed from the United States at any time. Although 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:

Information contained in this system of records includes, but is not limited to:

- Biographic data, such as:
    - Name;
    - Date of birth;
    - Nationality;
    - Social Security number (SSN), when available; and
    - Other personal descriptive data.
- Biometric indicator data, which includes, but is not limited to:
    - Fingerprint identification numbers (FIN);[1] and
    - Encounter identification numbers (EID).
- System-generated identification numbers: ADIS holds data from other DHS and federal agency systems, and identifies/points to the source systems of these records.
- Encounter data, such as:
    - Encounter location;
    - Arrival and departure dates;
    - Flight information;

[1] Currently, DHS assigns a Fingerprint identification number (FIN) to collected iris images.

- Immigration status changes;
- Document types;
- Document numbers;
- Document issuance information;
- Address while in the United States; and
- Narrative information entered by immigration enforcement officers, such as references to:
  - Active criminal immigration enforcement investigations;
  - Immigration enforcement investigations;
  - Immigration status information; and
  - Details from law enforcement or security incidents or encounters.

- Entry or exit data 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, 1373, 1379, and 1732.

Purpose(s):

The purpose of this system is to serve as the primary repository for tracking entry and exit data throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes. This data is collected by DHS or other federal or foreign

government agencies and is used in connection with DHS missions such as 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, DHS/CBP uses ADIS data to: (1) 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, ability to receive or renew a U.S. visa, or to receive governmental benefits); (2) 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 (3) 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 consistent with a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys,

or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The U.S. or any agency thereof.

B. 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.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations of the system as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has 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 identity theft or fraud, harm to economic or property

interests, harm to an individual, 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 made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To appropriate federal, state, tribal, local, international, or foreign law enforcement agencies or other appropriate authorities charged with investigating or prosecuting a violation of or enforcing or implementing a law, rule, regulation, or order, when CBP believes the information would assist enforcement of applicable civil and criminal laws, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. 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.

I. 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, retention, or vetting by such an agency of an employee, contractor, or visitor; the issuance of a security clearance; the granting of clearance to access a secure facility; the auditing of compliance with any terms of employment or 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.

J. 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.

K. 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.

L. To approved federal, state, and local government agencies for any legally mandated purpose in accordance with an authorizing statute and when an approved Memorandum of Agreement or Computer Matching Agreement (CMA) is in place between DHS and the agency.

M. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Disclosure to consumer reporting agencies:

None.

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

Storage:

DHS/CBP stores records electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

Retrievability:

DHS/CBP retrieves records using 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:

DHS/CBP safeguards records in this system according to applicable rules and

policies, including all applicable DHS automated systems security and access policies. DHS/CBP imposes strict controls 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 CBP Records Office and the 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, CBP, U.S. Department of Homeland Security, Washington, D.C. 20229-1038.

Notification procedure:

The Secretary of Homeland Security 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/CBP 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 CBP Freedom of Information

Act (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 FOIA Officer, Department of Homeland Security, 245 Murray Drive S.W., Building 410, STOP-0655, Washington, D.C. 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 FOIA 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.

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:

DHS/CBP obtains records about individuals covered by this system directly and by 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 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).

When this system receives a record from another system exempted in that source system under 5 U.S.C. § 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claim any additional exemptions set forth here.

Jonathan R. Cantor
Deputy Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2015-29445 Filed: 11/17/2015 8:45 am; Publication Date: 11/18/2015]