BILLING CODE 4410-10

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

DHS-2005-0040

Privacy Act of 1974; Systems of Records

AGENCY: Privacy Office; Department of Homeland Security

ACTION: Notice of Privacy Act system of records.

SUMMARY: The Department of Homeland Security is creating a new system of records for the United States Visitor and Immigrant Status Indicator Technology Program. This new system of records is the Automated Identification Management System. It will be used to facilitate and further automate processes for entry into and exit from the United States through the issuance, to covered individuals, of a radio frequency identification tag with a unique identifier. These tags and their associated reading, processing, and storage components are intended to improve the recording of entry and exit data at U.S. land border Ports of Entry beginning July 31, 2005.

DATES: The new system of records will be effective July 31, 2005, unless comments are received that result in a contrary determination.

ADDRESSES: You may submit comments, identified by EPA DOCKET NUMBER DHS-2005-0040 by one of the following methods:

- EPA Federal Partner EDOCKET Web Site: http://www.epa.gov/feddocket. Follow instructions for submitting comments on the web site.

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: (202) 298-5201.
- Mail: Steve Yonkers, US-VISIT Privacy Officer, 245 Murray Lane, SW, Washington, DC 20538; Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 601 S. 12th Street, Arlington, VA 22202-4220.

FOR FURTHER INFORMATION CONTACT: Steve Yonkers, US-VISIT Privacy Officer, 245 Murray Lane, SW, Washington, DC 20538, by telephone (202) 298- 5200 or by facsimile (202) 298-5201.

SUPPLEMENTARY INFORMATION:

The Department of Homeland Security (DHS) has established the United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT), an integrated, automated entry-exit system that records the arrival and departure of covered individuals; verifies their identities and authenticates their travel documents through comparison of biometric identifiers. Individuals subject to US-VISIT are required to provide finger scans, photographs, or other biometric identifiers upon arrival in, or departure from, the United States.

US-VISIT has been implemented in increments. As part of Increment 2, US-VISIT will test the use of passive radio frequency identification (RFID) tags to automatically, passively, and remotely record the entry and exit of covered individuals. These RFID tags will be embedded in the Form I-94 or I-94W, which is an Arrival-Departure Record issued to a traveler. The RFID tag, which

will contain a unique identification code, will be linked at a POE with the biographic and biometric information that was collected when the traveler entered the United States.

When travelers either drive or walk through the port-of-entry, a transceiver will send out a harmless radio wave frequency that will power the DHS-issued RFID tag to transmit back a unique identifier code number. This code number, when received by the transceiver, will be relayed back to secure DHS computer systems and matched with the biographic and/or biometric data of the traveler. The RFID tag number will not contain or be derived from any personal information. DHS will be able to automatically identify and document the exits and, if applicable, the subsequent re-entry of covered individuals.

To collect, store, and maintain the unique RFID tag number and the matching biographic and/or biometric data, US-VISIT is creating a new Privacy Act system of records, the Automated Identification Management System (AIDMS).

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. 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 the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system to make agency recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency. Individuals may request their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations (6 CFR 5.21).

US-VISIT is hereby publishing the description of the AIDMS system of records. In accordance with 5 U.S.C. 552a(r), a report of this new system of records has been provided to the Office of Management and Budget (OMB) and to the Congress.

DHS/US-VISIT 001

SYSTEM NAME:

Department of Homeland Security (DHS), United States Visitor and Immigration Status Indicator Technology, Automated Identification Management System (AIDMS).

SYSTEM LOCATION:

The primary AIDMS records database is located at the DHS Data Center in Ashburn, Virginia. AIDMS interfaces, RFID tag readers, and other supporting components are located at U.S. land border Ports of Entry (POE).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by the system ("covered individuals") consist of aliens as that term is defined in section 101(a)(3) of the Immigration and Nationality Act (INA): any person not a citizen or national of the United States.

CATEGORIES OF RECORDS IN THE SYSTEM:

The AIDMS maintains four general categories of records: traveler (i.e., covered individual) identification information, RFID tag related information, RFID tag read event information, and border crossing history information.

1. Traveler identification information includes the AIDMS unique traveler identification number (i.e., the traveler's RFID tag number); and data received from the TECS database within Customs and Border Protection (CBP). The data received from TECS was collected as part of the form I-94 and form I-94W issuance process and may include: the traveler's complete name; date of birth; and travel document type (e.g., visa), number, date, and country of issuance.

2. RFID tag related information encompasses data collected about the issuance and status and may include: RFID tag number; status (e.g., active, returned, seized, lost or stolen, damaged, location, date/time, identification number of the CBP officer responsible for the transaction).

3. RFID tag read event information is transactional data associated with the reading of an RFID tag and may include: RFID tag number associated with a read event; transaction identification numbers; type, date/time and location of a read event; direction of border crossing (entry or exit); and equipment identification numbers involved in the read event.

4. Border crossing history information consists of the composition of information from the other three categories of information into a border crossing event that is communicated to other DHS systems which support the US-VISIT Program, such as TECS and the Arrival and Departure Information System (ADIS).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. 1187, 1221, 1722, 1731

PURPOSE (S) OF THE SYSTEM:

The AIDMS system will provide the capability to automatically, passively, and remotely record the entry and exit of covered individuals using Radio Frequency Identification (RFID) tags. The RFID tag will be embedded in the I-94 Arrival/Departure forms, and will use a unique ID number embedded in the tag to associate the data on the form I-94 with the tag. After the tag-enabled form I-94 is issued to an individual, the ID number will be used as a pointer to the individual's biographic information located in the TECS database maintained by CBP. Biometric information, if applicable, is contained in the Automated Biometric Identification System (IDENT) maintained by US-VISIT. When the individual passes through the entry and exit lanes of a POE, the ID number will be read and used to retrieve the individual's immigration information for use in the entry and exit inspection processes by CBP officers.

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 government agencies or organizations (regardless of whether they are federal, state, local, foreign, or tribal), lawfully engaged in collecting law enforcement (whether civil, criminal, or administrative) or intelligence information and/or charged with investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders, to enable these entities to carry out their law enforcement and intelligence responsibilities.

B. In a proceeding before a court, grand jury, or adjudicative body when records` are determined by the Department of Homeland Security to be arguably relevant to the proceeding where any of the following is a party: (1) the DHS, or any DHS component, or subdivision thereof; (2) any DHS employee in his or her official capacity; (3) any DHS employee in his or her individual capacity when the DHS has agreed to represent the employee or has authorized a private attorney to represent him or her; and (4) the United States, where the DHS or its components are likely to be affected.

C. To a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

D. To the National Archives and Records Administration or other federal government agencies in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

E. To the news media and the public when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of the Department or is necessary to demonstrate the accountability of the Department's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

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 an agency function related to this system of records.

G. To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

AIDMS electronic records are temporarily stored in systems (including, but not limited to, electronic readers, databases, servers, workstations, and message queues) at land border POEs and at principally stored at the primary AIDMS records database at the DHS Data Center in Ashburn, Virginia.

RETRIEVABILITY:

Information may be searched and retrieved based on various data elements, including, but not limited to: RFID tag number, traveler identification number, transaction number, and name of covered individual.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws and policies, including the DHS Information Technology Security Program Handbook. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. The system is also protected through a multi-layer security approach. The protective strategies are physical, technical, administrative and environmental in nature and provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to

ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

RETENTION AND DISPOSAL:

The information that resides in the AIDMS is temporary and is retained only as long as needed to process a covered individual's land border crossing and to transfer the crossing information to existing DHS systems. US-VISIT is working with the U.S. National Archives and Records Administration (NARA) to develop a retention schedule.

SYSTEM MANAGER(S) AND ADDRESS:

Program Manager, AIDMS Program Management Office, US-VISIT Program, Border and Transportation Security, U.S. Department of Homeland Security, Washington, D.C. 20528, USA.

NOTIFICATION PROCEDURES:

To determine whether this system contains records relating to you, write to the US-VISIT Privacy Officer, US-VISIT Program, Border and Transportation Security, U.S. Department of Homeland Security, 245 Murray Lane SW, Washington, D.C. 20528, USA.

RECORD ACCESS PROCEDURES:

Requests for access, confirmation, or data correction must be in writing and should be addressed to the US-VISIT Privacy Officer above. Requests should conform to the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope

and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

CONTESTING RECORD PROCEDURES:

Same as "Notification Procedures" and "Record Access Procedures," above.

RECORD SOURCE CATEGORIES:

The records in this system come directly from the RFID tag embedded in the I-94 Arrival/Departure forms, information located in the TECS database maintained by CBP, and information captured directly from the covered individual. Each RFID tag will use a unique ID number embedded in the tag to associate the I-94 holders with the tag. After the tag-enabled I-94 is issued to an individual, the ID number will be used as a pointer to the individual's biographic information located in the TECS database. When the individual passes through the entry and exit lanes of a POE, the ID number will be read and used to retrieve the individual's immigration information for use in the entry and exit inspection processes by CBP officers.

EXEMPTIONS CLAIMED FOR THE SYSTEM: None.

Dated:

Nuala O'Connor Kelly
Chief Privacy Officer.