9111-28

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0053]

Privacy Act of 1974; Department of Homeland Security/ICE- 015 LeadTrac System of Records

AGENCY: Department of Homeland Security (DHS), 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 establish a new DHS system of records titled, "DHS/ICE-015 LeadTrac System of Records." This new system of records is being created from a previously issued system of records, DHS/ICE 009-External Investigations SORN. 73 FR 75452 (Dec. 11, 2008). This system of records allows DHS to collect and maintain records gathered by and in the possession of U.S. Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Counterterrorism and Criminal Exploitation Unit (CTCEU) and ICE field offices for appropriate enforcement action, used in the course of their duties in identifying, investigating, and taking enforcement action against foreign students, exchange visitors, and other non-immigrant visitors to the United States who overstay their period of admission or otherwise violate the terms of their visa, immigrant, or non-immigrant status (collectively, status violators) through the LeadTrac system. This SORN also allows DHS to collect information in LeadTrac about organizations such as schools, universities, and exchange visitor

programs being investigated by CTCEU and information about individuals, including designated school officials (DSOs), and associates of suspected status violators.

Additionally, DHS/ICE is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This newly established system will 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 new 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-2016-0053 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. 20528-0655.

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: Amber Smith, Privacy Officer, (202) 732-3300, U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536, e-mail: ICEPrivacy@dhs.gov. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

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. Immigration and Customs Enforcement (ICE) proposes to establish a new DHS system of records titled, "DHS/ICE–-015 LeadTrac System of Records."

This record system allows DHS to collect and maintain information about foreign students, exchange visitors, and other non-immigrant visitors to the United States, as well as associated organizations and individuals, who overstay their period of admission or otherwise violate the terms of their visa, immigrant, or non-immigrant status (collectively, "status violators"). Using the LeadTrac information technology (IT) system, ICE Homeland Security Investigations (HSI), Counterterrorism and Criminal Exploitation Unit (CTCEU) collects PII from key DHS databases and analyzes it to identify suspected status violators. This system of records contains records from Arrival and Departure Information System (ADIS), Student and Exchange Visitor Information System (SEVIS), Enforcement Integrated Database (EID/ENFORCE), TECS, Consular

Consolidated Database (CCD), Computer - Linked Application Information Management System (CLAIMS 3), Automated Biometric Identification System (IDENT), and from commercial databases and public sources. CTCEU will also use LeadTrac to collect information about organizations such as schools, universities, and exchange visitor programs being investigated by CTCEU, and information about individuals, including designated school officials (DSOs) and associates of suspected status violators.

ICE collects information in LeadTrac about suspected status violators and organizations to help enforce compliance with U.S. immigration laws. Specifically, the information is collected and used to support the following DHS activities: investigating and determining immigration status of individuals; identifying fraudulent schools and/or organizations and the people affiliated with those schools or organizations; providing HSI and Enforcement and Removal Operations (ERO) with information to further investigate suspected status violators; and carrying out the required enforcement activity.

Some of the individuals about whom ICE collects information in LeadTrac, such as DSOs and associates of suspected status violators, may have lawful permanent resident (LPR) status or be U.S. citizens. CTCEU and Overstay Analysis Unit (OAU) personnel query a variety of DHS and non-DHS information systems and enter the results into LeadTrac to build a unified picture of an individual's entry/exit, visa, criminal, and immigration history, and will comparably process information about associated individuals and organizations. Using this assembled information, CTCEU personnel will determine which individuals and organizations warrant additional investigation for

possible status violations or the operation of fraudulent institutions, and will request that the appropriate HSI field offices initiate investigations.

Consistent with the Department's information sharing mission, information stored in the DHS/ICE-015 LeadTrac System of Records 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, DHS/ICE may share information 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.

Additionally, DHS/ICE is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

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.

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. Immigration Customs Enforcement (ICE)-015

System name:

DHS/ ICE-015 LeadTrac System of Records

Security classification:

Unclassified; Law Enforcement Sensitive.

System location:

DHS/ICE maintains records at the U.S. Immigration and Customs Enforcement (ICE) Headquarters in Washington, D.C. and field offices. Specifically, all records are maintained in the LeadTrac information technology (IT) system, except an extract of records from the legacy LeadTrac system that is maintained in an archived electronic form and stored at the National Archives and Records Administration's (NARA) Federal Records Center.

Categories of individuals covered by the system:

Categories of individuals covered by this system include: (1) individuals who are suspected of overstaying their period of admission, have had their visa revoked, or otherwise violate the terms of their visa, immigrant, or non-immigrant status (suspected

status violators). This includes foreign students, exchange visitors, dependents, and other visitors to the United States; (2) associates of suspected status violators, including family members and employers, who may include U.S. citizens; (3) Designated School Officials (DSOs) and other individuals involved in the operation of suspected status violators' institutions; and (4) Chief executives and legal counsel of Student and Exchange Visitor Program (SEVP)-certified schools, and designated exchange visitor sponsors.

Categories of records in the system:

For individuals who are suspected status violators:

1) Biographic and other identifying information, to include but not limited to names, dates of birth, countries of birth, countries of citizenship, gender, Social Security number (SSN), financial information, and vehicle information;
2) Travel-related data, such as passport and visa information and other information related to entry and exit of the United States;
3) Education data, which may include program of study, school name, school type, school address, school telephone number, school code, enrollment information, Student and Exchange Visitor Information System (SEVIS) certification date, accreditation information, and school operating authority; and
4) DHS immigration benefit applications data filed with U.S. Government agencies, and data concerning matriculation at a U.S. college or university, employment, civil litigation, and/or criminal history.

For a suspected status violator's associates and family members: names, dates of birth, contact information, and other identifying numbers.

For school and exchange visitor officials: names, SEVIS ID numbers, aliases, gender, dates of birth, countries of birth and citizenship, contact information, and identifying numbers, which may include, but are not limited to alien number and passport number.

Authority for maintenance of the system:

Pursuant to the Homeland Security Act of 2002 (Pub. L.107-296, Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include, but are not limited to, laws residing in titles 8, 18, 19, 21, 22, 31, and 50 of the U.S.C. The Secretary delegated this authority to ICE in DHS Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003).

Purpose(s):

LeadTrac is owned by the U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU). The purpose of this system is to identify and vet visitors to the United States who overstay their period of admission or otherwise violate the terms of their visa, immigrant or non-immigrant status. LeadTrac also vets, collects, and maintains information on organizations such as schools, universities, and exchange visitor programs being investigated by CTCEU.

Specifically, the information is collected and used to support the following DHS activities: investigating and determining immigration status and criminal history information about individuals and carrying out the required enforcement activity; determining the likelihood of, or confirming a suspected violator's continued presence within the United States and assessing the associated risk level; identifying fraudulent schools and/or organizations and the people affiliated with those schools or organizations; and providing HSI and Enforcement and Removal Operations (ERO) with information to further investigate suspected status violators and carry out the required enforcement activity.

This system of records also supports the identification of potential criminal activity, immigration violations, and threats to homeland security. The system is used to uphold and enforce the law, and to ensure public safety.

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 the DOJ, including Offices of the United States Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when disclosure 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 United States 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 NARA or the 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 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, local, tribal, territorial, international, or foreign law enforcement agencies or other appropriate authorities charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, rule, regulation, or order, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To Federal, State, local, tribal, territorial, foreign or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an

investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit.

I. To Federal, State, local, tribal, territorial, international, or foreign criminal, civil, or regulatory law enforcement authorities when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

J. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

K. To Federal, State, local, tribal, territorial, foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

L. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property.

M. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure

is appropriate to the proper performance of the official duties of the officer making the disclosure.

N. 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/ICE stores records in this system 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/ICE may retrieve records by biographic information, identifying numbers, and by other key data elements contained in the system.

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 permission.

Retention and disposal:

Under the NARA-approved records retention schedule for LeadTrac, records must be retained for 75 years. ICE intends to request NARA approval to retain LeadTrac records for 25 years from the date the record was created. Under this schedule, records would be kept as active in LeadTrac for 20 years, and archived for an additional five-year period. After the 25-year period, the information would be destroyed or, if deemed necessary, retained further under a reset retention schedule.

System Manager and address:

Section Chief, Counterterrorism and Criminal Exploitation Unit (CTCEU), Homeland Security Investigations, U.S. Immigration and Customs Enforcement, 1515 Wilson Boulevard, Arlington, VA 22209.

Notification procedure:

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 ICE's Freedom of Information Act (FOIA) Officer or the Chief Privacy 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, 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 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.

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:

Individuals who wish to contest the accuracy of records in this system of records should submit these requests to the ICE Office of Information Governance and Privacy. Requests must comply with verification of identity requirements set forth in Department of Homeland Security Privacy Act regulations at 6 CFR 5.21(d). Please specify the nature of the complaint and provide any supporting documentation. By mail (please note substantial delivery delays exist): ICE Office of Information Governance and Privacy, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536. By email: ICEPrivacy@ice.dhs.gov. Please contact the Office of Information Governance and Privacy with any questions about submitting a request or complaint at 202-732-3300 or ICEPrivacy@ice.dhs.gov.

Record source categories:

Records are obtained from key DHS systems of records to include but not limited to:

- Arrival and Departure Information System (ADIS). 80 FR 72,081 (November 18, 2015).
- Student and Exchange Visitor Information System (SEVIS). 75 FR 412 (January 5, 2010).

- Enforcement Integrated Database (EID/ENFORCE). 80 FR 24,269 (April 30, 2015).
- TECS (not an acronym). 73 FR 43,457 (July 25, 2008).
- Benefits Information Systems (BIS). 73 FR 56,596 (September 29, 2008).
- Automated Biometric Identification System (IDENT). 72 FR 31,080 (June 5, 2007).

Records are also obtained from the U.S. Department of State's Consular Consolidated Database (CCD) (77 FR 65,245 (Oct. 25, 2012)), commercial databases, and public sources.

Exemptions claimed for the system:

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2) has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2) or (k)(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 claims any additional exemptions set forth here.

Dated: August 3, 2016

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-18810 Filed: 8/8/2016 8:45 am; Publication Date: 8/9/2016]