



## DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2016-0087]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Immigration and Customs Enforcement-015 LeadTrac System of Records

**AGENCY:** Privacy Office, Department of Homeland Security.

**ACTION:** Final rule.

**SUMMARY:** The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a newly established system of records titled,

“Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE)-015 LeadTrac System of Records” from certain provisions of the Privacy Act.

Specifically, the Department exempts portions of the “DHS/ICE-015 LeadTrac System of Records” from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

**DATES:** This final rule is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**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@ice.dhs.gov](mailto:ICEPrivacy@ice.dhs.gov). For privacy issues, please contact: Jonathan R. Cantor (202-

1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

## **SUPPLEMENTARY INFORMATION:**

### **Background**

DHS/ICE published a notice of proposed rulemaking in the Federal Register, 81 FR 153, August 9, 2016, proposing to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The system of records is the DHS/ICE - 015 LeadTrac System of Records. The DHS/ICE-015 LeadTrac System of Records Notice was published concurrently in the Federal Register, 81 FR 153, August 9, 2016, and comments were invited on both the Notice of Proposed Rulemaking (NPRM) and System of Records Notice (SORN).

### **Public Comments**

DHS received no comments on the NPRM and no comments on the SORN.

Because DHS received no public comments, the Department will implement the rulemaking as proposed.

### **List of Subjects in 6 CFR Part 5**

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

### **PART 5--DISCLOSURE OF RECORDS AND INFORMATION**

1. The authority citation for part 5 continues to read as follows:

**Authority:** Pub. L. 107-296, 116 Stat. 2135; (6 U.S.C. 101 *et seq.*); 5 U.S.C. 301.

Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. Add paragraph 75 to appendix C to part 5 to read as follows:

**Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act**

\* \* \* \* \*

75. The DHS/ICE-015 LeadTrac System of Records consists of electronic and paper records and will be used by ICE investigative and homeland security personnel. The DHS/ICE-015 LeadTrac System of Records is a repository of information held by ICE for analytical and investigative purposes. The system is used to conduct research supporting the production of law enforcement activities; provide lead information for investigative inquiry and follow-up; assist in the conduct of ICE criminal and administrative investigations; assist in the disruption of terrorist or other criminal activity; and discover previously unknown connections among existing ICE investigations. The DHS/ICE-015 LeadTrac System of Records contains aggregated data from ICE and DHS law enforcement and homeland security IT systems, as well as data uploaded by ICE personnel for analysis from various public, private, and commercial sources during the course of an investigation or analytical project. 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.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Disclosure of corrections or notations of dispute may impede investigations by requiring DHS to inform each witness or individual contacted during the investigation of each correction or notation pertaining to information provided them during the investigation.
- (b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that

investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose classified and other security-sensitive information that could be detrimental to homeland security.

- (c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.
- (d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.
- (e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

- (f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise establishing procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.
- (g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.
- (h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: November 17, 2016.

Jonathan Cantor,  
Acting Chief Privacy Officer,  
Department of Homeland Security.

[FR Doc. 2016-28289 Filed: 11/23/2016 8:45 am; Publication Date: 11/25/2016]