Proposed Rules

Federal Register
Vol. 71, No. 144
Thursday, July 27, 2006

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 5

[Docket No. DHS–2006–0035]

Privacy Act of 1974: Implementation of Exemptions

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a revised and updated system of records pursuant to the Privacy Act of 1974 for the Automated Biometric Identification System. In this proposed rulemaking, the Department proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before August 28, 2006.

ADDRESSES: You may submit comments, identified by docket number DHS–2006–0035, by one of the following methods:

- 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; Maureen Cooney, Acting Chief Privacy Officer, Department of Homeland Security, 601 S. 12th Street, Arlington, VA 22202–4220.

Instructions: All submissions received must include the agency name and docket number for this notice. 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, go to *http://www.regulations.gov.*

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:

Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) is publishing a revision to existing Privacy Act systems of records known as Enforcement Operational Immigration Records/Automated Biometric Identification System (ENFORCE/IDENT) in today's edition of the **Federal Register**. This proposed rule would exempt certain records from the access and amendment provisions of law as permitted by the Privacy Act.

ENFORCE is the primary administrative case management system for Immigration and Customs Enforcement (ICE). IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws (including the immigration law); investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. IDENT is a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context. 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.

For business purposes these two systems were operated jointly. Now, as a part of operational and technical restructuring, these systems will be operated independently—IDENT under the management of US–VISIT and ENFORCE under the management of ICE. Consequently, the ENFORCE/IDENT system notice is being split into two system notices: One for ENFORCE and one for IDENT. The Privacy Act notice for ENFORCE/IDENT was last published in the **Federal Register** on March 20, 2006 (71 FR 13987). In this notice of proposed rulemaking, DHS now is proposing to exempt IDENT, in part, from certain provisions of the Privacy Act.

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. 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 part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description of the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals in finding such files within the agency.

The Privacy Act allows Government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemption from certain requirements of the Privacy Act for IDENT. Some information in IDENT relates to official DHS national security, immigration and border management, and law enforcement activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and of immigration and border management and law enforcement personnel; to ensure DHS's ability to obtain

information from third parties and other sources; to protect the privacy of third parties; and to safeguard classified information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

The exemptions proposed here are standard law enforcement and national security exemptions exercised by a large number of Federal law enforcement and intelligence agencies. In appropriate circumstances, where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived.

List of Subjects in 6 CFR Part 5

Privacy, Freedom of information.

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. Amend Appendix C to part 5 by adding the following new paragraph 6:

Appendix C—DHS Systems of Records Exempt From the Privacy Act

* * * * *

6. The Department of Homeland Security Automated Biometric Identification System (IDENT) consists of electronic and paper records and will be used by DHS and its components. IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions and functions, including, but not limited to: the enforcement of civil and criminal laws (including the immigration law); investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. IDENT is a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context. 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.

Pursuant to exemptions 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt 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) and (e)(8); (f)(2) through (5); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), and (e)(4)(H). 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 the 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.

(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 the 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 impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose 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 an investigation, thereby interfering with the related investigation and law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G) and (H) (Agency Requirements), and (f)(2 through 5) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) and thereby would not require DHS to establish requirements or rules for records which are exempted from access.

(g) From subsection (e)(5) (Collection of Information) because in 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 (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' 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) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: July 16, 2006.

Maureen Cooney,

Acting Chief Privacy Officer.

[FR Doc. E6–11996 Filed 7–26–06; 8:45 am]

BILLING CODE 4410–10–P