Proposed Rules

Federal Register

Vol. 73, No. 160

Monday, August 18, 2008

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

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2007–0055]

Privacy Act of 1974: Implementation of Exemptions; Fraud Detection and National Security Data System (FDNS–DS) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is concurrently establishing a new system of records pursuant to the Privacy Act of 1974 entitled the Technical Fraud Detection and National Security Data System (FDNS–DS). The USCIS has developed the Fraud Detection and National Security Data System (FDNS–DS), a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns. 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 September 17, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2007–0055, by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 1–866–466–5370.
- *Mail:* Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *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 go to *http://www.regulations.gov*.

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: For general questions please contact: United States Citizenship and Immigration Services, Privacy Officer, Donald Hawkins 111 Massachusetts Avenue, NW., Washington, DC 20529. For privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Office of Fraud Detection and National Security (FDNS) of the United States Citizenship and Immigration Services (USCIS) has developed a new system named the Fraud Detection and National Security Data System (FDNS–DS). FDNS–DS is a central repository that permits specially-trained employees to record, track, and manage the background check and adjudicative processes related to immigration applications and petitions with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments (BFAs). The system will also have the capability to track the following:

1. USCIS investigative referrals to law enforcement agencies (LEAs);
2. LEA referrals to USCIS concerning subjects with pending immigration benefit applications or petitions;
3. background check referrals and resolutions associated with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns; and
4. any additional inquiries conducted in order to confirm that the information on file is correct.

FDNS has created FDNS–DS, a centralized data system, in order to increase the effectiveness of the United States (U.S.) immigration system in identifying threats to national security, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system. With the implementation of FDNS–DS, USCIS's capabilities for detecting and tracking benefit fraud and other criminal activity—and conducting efficient and accurate background check resolutions and adjudication of national security cases will be increased.

In order to achieve the goals discussed above, FDNS–DS will store data related to immigration applications involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns. The data will include the results of required background checks conducted in connection with pending petitions/applications that result in subsequent inquiries conducted to resolve the background check results. FDNS–DS will also contain the following information related to cases involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns: USCIS investigative referrals to law enforcement agencies (LEAs) of suspected or confirmed fraud or other criminal activity; LEA referrals to USCIS related to pending applications; referrals to USCIS from the public or other governmental entities or fraud case referrals from the Benefit Fraud Assessment (BFA) process (''other referrals''); adverse information identified by USCIS from applications, administrative files, interviews, written requests for evidence (RFEs) or site visits; results of resolution of any of the above-described categories of adverse information; and adjudicative summaries and decisions.

FDNS–DS will store information concerning cases randomly selected for BFAs and will track interactions with Immigration and Citizenship Enforcement (ICE) and other LEAs (e.g., the Federal Bureau of Investigation [FBI], the Drug Enforcement

Administration [DEA], and U.S. Customs and Border Protection [CBP]) in cases involving fraud or other criminal activity, and the Department of State in cases involving fraud related to selected types of visas for entry into the United States.

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.

In this Notice of Proposed Rulemaking, DHS now is proposing to exempt FDNS–DS, in part, from certain provisions of the Privacy Act. Some information in FDNS–DS relates to official DHS law enforcement, intelligence, and immigration 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; and to protect the privacy of third parties. 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

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. At the end of appendix C to part 5, add the following new paragraph ''7'':

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

* * * * *

7. The Department of Homeland Security United States Citizenship and Immigration Services Fraud Detection and National Security Data System (FDNS–DS) System of Records consists of a stand-alone database and paper files that will be used by DHS and its components. FDNS–DS is a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns.

The Secretary of Homeland Security has exempted this system from 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), 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(k)(2). 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) (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 subsections (e)(4)(G) and (e)(4)(H) (Agency Requirements) because portions of this system are exempt from the individual access provisions of subsection (d) which exempts providing access because it could alert a subject to the nature or existence of an investigation, and thus there could be no procedures for that particular data. Procedures do exist for access for those portions of the system that are not exempted.

(e) From subsection (e)(4)(I) (Agency Requirements) because providing such source information would impede law enforcement or intelligence by compromising the nature or existence of a confidential investigation.

(f) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

Dated: August 11, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–19034 Filed 8–15–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF AGRICULTURE

Agricultural Marketing Service

7 CFR Part 922

[Docket No. AMS–FV–08–0052; FV08–922–1 PR]

Apricots Grown in Designated Counties in Washington; Increased Assessment Rate

AGENCY: Agricultural Marketing Service, USDA.

ACTION: Proposed rule.

SUMMARY: This rule would increase the assessment rate established for the Washington Apricot Marketing Committee (Committee) for the 2008–09 and subsequent fiscal periods from $1.50 to $2.00 per ton for Washington apricots. The Committee is responsible for local administration of the marketing order regulating the handling of apricots grown in designated counties in Washington. Assessments upon handlers of apricots are used by the Committee to fund reasonable and necessary expenses of the program. The fiscal period for the marketing order begins April 1 and ends March 31. The assessment rate would remain in effect indefinitely unless modified, suspended or terminated.

DATES: Comments must be received by September 2, 2008.