Proposed Rules

Federal Register
Vol. 78, No. 13
Friday, January 18, 2013

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 2012–0076]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security U.S. Customs and Border Protection—002 Global Enrollment System (GES), System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of an updated and reissued system of records pursuant to the Privacy Act of 1974 for the ''Department of Homeland Security/U.S. Customs and Border Protection—002 Global Enrollment System (GES), System of Records'' and this proposed rulemaking. In this proposed rulemaking, the Department proposes 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.

DATES: Comments must be received on or before February 19, 2013.

ADDRESSES: You may submit comments, identified by docket number DHS 2012–0076, 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, DC 20528.

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: Laurence Castelli, (202) 325–0280, CBP Privacy Officer, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street NW., Washington, DC 20229. For privacy issues please contact: Jonathan R. Cantor (202–343–1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

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. Customs and Border Protection (CBP) proposes to exempt portions of a current DHS system of records titled, ''DHS/CBP–002 Global Enrollment System (GES)'' system of records.

Global Entry (GE) is the DHS/CBP program that enables CBP to expedite the inspection and security process for lower risk travelers and allows more scrutiny for those travelers who present an unknown risk. GE, previously a pilot program, is now a permanent trusted traveler program (77 FR 5681 (Feb. 6, 2012)). Under GE, expedited processing into the United States and certain foreign countries will be expanded through a growing number of participating U.S. and foreign international airports and foreign partnerships. Through such partnerships, U.S. citizens and citizens of certain foreign countries will be able to apply for expedited processing at their respective airports.

CBP has signed a number of joint statements with foreign partners that provide the basic framework for allowing U.S. citizens and citizens of the applicable foreign countries to apply for expedited processing at their respective airports. The general purpose of the joint statement is to offer expedited processing to U.S. citizens and the citizens of the foreign country that is party to that joint statement, based on a mutually determined set of vetting criteria and standards. CBP continues to work with government border authorities in various countries to create this growing international network in which, once individuals are screened and deemed trusted by the authorities in their own country, the other country in the alliance will accept them in their respective national trusted traveler programs.

In addition to new foreign partners, CBP has consolidated the registered traveler programs under GES to include the Small Vessel Reporting System (SVRS) and the Decal and Transponder Online Procurement System (DTOPS). SVRS, as an enhancement to the Local Boater Option (LBO) pilot program, allows individuals with advance submission and CBP approval of float plans to use a designated telephone line to notify a CBP officer of their arrival to the United States. DTOPS is a registered traveler program that allows individuals to purchase, renew, or transfer user fees related to the transponders/Radio Frequency Identification (RFID) tags for their commercial vehicles or to the decals for their private aircraft or vessels in advance of crossing a U.S. border.

The system of records notice is being re-published to update the categories of records, authorities, purposes, routine uses, retrievability, retention and disposal, notification procedures, record sources, and Privacy Act exemptions for the system of records. Specifically, DHS is updating the category of records to clarify that GES maintains limited law enforcement information, consisting of the case number references to law enforcement databases used to support or deny the membership decision for GES trusted traveler programs, as well as the membership decision for trusted traveler programs with foreign partners. These results were previously covered by the DHS/CBP–011 TECS SORN (73 FR 77778 (Dec. 19, 2008.) DHS/CBP is also retaining the fact of the other foreign governments' decisions either to approve or deny an application, pursuant to the applicable joint statements.

Participation in these programs is entirely voluntary. Joint statements with foreign partners establish that each country's use of GES information for vetting will be consistent with applicable domestic laws and policies. Participants should be aware that when they submit their information to a foreign country, or agree to share their information with a foreign partner, the foreign country uses, maintains, retains, or disseminates their information in accordance with that foreign country's laws and privacy protections.

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted the law enforcement related records, including the pointer information to other law enforcement databases that support the DHS/CBP membership decision, and the law enforcement risk assessment worksheet that have been created during the background check and vetting process, from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted records created during the background check and vetting process from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). In addition, when a record contains information from other exempt systems of records, DHS/CBP will claim the same exemptions for that record as are claimed for the original systems of records, and will claim any additional exemptions provided here.

CBP will not assert any exemptions with regard to accessing or amending an individual's application data and final membership determination in the trusted traveler program. However, this data may be shared with law enforcement and/or intelligence agencies pursuant to the routine uses identified in this SORN. The Privacy Act requires DHS maintain an accounting of such disclosures made pursuant to all routine uses. Disclosing the fact that a law enforcement and/or intelligence agency has sought particular records may affect ongoing law enforcement activity. As such, the Secretary of Homeland Security pursuant to 5 U.S.C. 552a (j)(2) and (k)(2), will claim an exemption from (c)(3), (e)(8), and (g)(1) of the Privacy Act, as is necessary and appropriate to protect this information. The updated system will be included in DHS'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 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. 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.

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 exemptions from certain requirements of the Privacy Act for DHS/CBP—002 GES. Some information in DHS/CBP—002 GES System of Records relates to official DHS national security, law enforcement, 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 or to avoid disclosure of activity techniques. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when 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 on a case by case basis.

A notice of system of records for DHS/CBP—002 GES System of Records is also published in this issue of the **Federal Register**.

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. In Appendix C to Part 5, revise paragraph ''68'', to read as follows:

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

* * * * *

68. The DHS/U.S. Customs and Border Protection (CBP)—002 Global Enrollment System (GES) system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/CBP–002 GES system of records collects and maintains records on individuals who voluntarily provide personally identifiable information to U.S. Customs and Border Protection in return for enrollment in a program that will make them eligible for expedited processing at designated U.S. border ports of entry. The DHS/CBP–002 GES system of records contains personally identifiable information in biographic application data, biometric information, conveyance information, pointer information to other law enforcement databases that support the DHS/CBP membership decision, Law Enforcement risk assessment worksheets, payment tracking numbers, and U.S. or foreign trusted traveler membership decisions in the form of a ''pass/fail.''

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted the law enforcement related records, including the pointer information to other law enforcement databases that support the DHS/CBP membership decision, and the law enforcement risk assessment worksheet that have been created during the background check and vetting process 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)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted records created during the background check and vetting process from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

CBP will not assert any exemptions with regard to accessing or amending an individual's application data in a trusted or registered traveler program and/or final membership determination in the trusted traveler programs. However, this data may be shared with law enforcement and/or intelligence agencies pursuant to the published routine uses in the system of records notice, DHS/CBP–002 GES. The Privacy Act requires DHS maintain an accounting of such disclosures made pursuant to all routine uses. Disclosing the fact that a law enforcement and/or intelligence agency has sought particular records may affect ongoing law enforcement activity. As such, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2) has exempted these records from (c)(3), (e)(8), and (g)(1) of the Privacy Act, as is necessary and appropriate to protect this information. When a record received from another system has been exempted in that source system, 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.

(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 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 setting up 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, and 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.

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

* * * * *

Dated: December 31, 2012.

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2013–00800 Filed 1–17–13; 8:45 am]

BILLING CODE 9111–14–P

FEDERAL ELECTION COMMISSION

11 CFR Part 111

[Notice 2013–01]

Request for Comment on Enforcement Process

AGENCY: Federal Election Commission.

ACTION: Request for comments.

SUMMARY: The Federal Election Commission is requesting comment on certain aspects of its enforcement process. First and foremost, the Commission welcomes public comment on whether this agency is doing an effective job in enforcing the Act and Commission regulations. Additionally, the Commission is currently reviewing and seeks public comment on: Its policies, practices, and procedures during the enforcement process stage set forth in 2 U.S.C. 437g(a)(1), prior to the Commission's determination of whether there is ''reason to believe'' that a person has committed, or is about to commit, a violation of the Federal Election Campaign Act of 1971, as amended, 2 U.S.C. 431 et seq. (''FECA'' or ''the Act'') and/or the Commission's implementing regulations; and the Commission's authority under 2 U.S.C. 437g(a)(5) to seek civil penalties from respondents pursuant to a finding of ''probable cause to believe'' that a respondent has violated the Act and/or Commission regulations, as well as the Commission's practice of seeking civil penalties prior to a finding of probable cause.

DATES: Comments must be received on or before Friday, April 19, 2013. The Commission will determine at a later date whether to hold a hearing.

ADDRESSES: All comments must be in writing. Comments may be submitted electronically via email to *process@fec.gov.* Commenters are encouraged to submit comments electronically to ensure timely receipt and consideration. Alternatively, comments may be submitted in paper form. Paper comments must be sent to the Federal Election Commission, Attn.: Commission Secretary, 999 E Street NW., Washington, DC 20463. All comments must include the full name and postal service address of the commenter, and of each commenter if filed jointly, or they will not be considered. The Commission will post comments on its Web site at the conclusion of the comment period.

FOR FURTHER INFORMATION CONTACT: Mr. Stephen A. Gura, Deputy Associate General Counsel for Enforcement, 999 E Street NW., Washington, DC 20463, (202) 694–1650 or (800) 424–9530.

SUPPLEMENTARY INFORMATION:

Background

I. Past Commission Hearings and Enforcement Process Reforms

The Commission is currently reviewing, and seeks public comment on, certain enforcement policies, practices, and procedures. The Commission will use the comments received to determine whether its policies, practices, or procedures should be adjusted, and whether rulemaking in these areas is advised. The Commission has made no decisions in these areas and may choose to take no action. The Commission last conducted a comprehensive review of its enforcement policies, practices, and procedures, among other issues, in late 2008 and early 2009. *See* Agency Procedures, 73 FR 74494 (Dec. 8, 2008). Comments filed in the 2008/2009 review, as well as a transcript of the public hearing, are available on the Commission's Web site at *http://www.fec.gov/law/policy/enforcement/publichearing011409.shtml.* Subsequent to that review, the Commission adopted or formalized several procedures