[Federal Register Volume 78, Number 11 (Wednesday, January 16, 2013)]

[Notices]

[Pages 3441-3446]

From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov/)]

[FR Doc No: 2013-00804]

=======================================================================

-----------------------------------------------------------------------

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0076]

Privacy Act of 1974; Department of Homeland/U.S. Customs and

Border Protection--002 Global Enrollment System (GES), System of

Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

-----------------------------------------------------------------------

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the

Department of Homeland Security proposes to update and reissue the

Department of Homeland Security system of records titled, ``Department

of Homeland Security/U.S. Customs and Border Protection--002 Global

Enrollment System'' system of records. This system of records allows

the Department of Homeland Security/U.S. Customs and Border Protection

to collect and maintain 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, including all trusted traveler and registered traveler programs.

This 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 exemptions sections of the system. Additionally, this

notice includes non-substantive changes to simplify the formatting and

text of the previously published notice. The Global Enrollment System

will now maintain law enforcement information as part of the vetting

results, therefore the Department of Homeland Security is issuing a

Notice of Proposed Rulemaking, to exempt this system of records from

certain provisions of the Privacy Act of 1974, as amended, elsewhere in

the Federal Register. This updated system will be included in the

Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before February 15, 2013. This updated

system will be effective February 15, 2013.

ADDRESSES: You may submit comments, identified by docket number DHS-

2012-0076 by one of the following methods:

[[Page 3442]]

 Federal e-Rulemaking Portal: [http://www.regulations.gov](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 rulemaking. All comments received will be

posted without change to [http://www.regulations.gov](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](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 questions, 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 update and reissue a current DHS system of

records titled, ``DHS/CBP-002 Global Enrollment System (GES).''

 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.

 Depending on the nature of the agreement with the foreign partner,

DHS/CBP will maintain and share different personally identifiable

information. In certain instances the joint statements commit to

allowing citizens of foreign countries to apply for GE after the

appropriate Interconnectivity Service Agreement (ISA) has been

implemented. In other instances, the joint statements commit to sharing

information about citizens who apply to be members of both countries'

trusted traveler program after the appropriate ISA has been

implemented. As part of the procedures for implementing a joint

statement and adding foreign partners to GE, CBP and each foreign

partner are executing parallel protocols that incorporate privacy

protections. A more in-depth discussion of the arrangements by country

is made available in DHS/CBP/PIA--002(b) GES Privacy Impact Assessment

and Appendix A ``CBP Global Entry Expansion: Joint Statements,'' which

is being published in conjunction with this system of records and will

be updated with relevant information.

 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.

 This 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 this 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.)) In cases when the applicant

has opted to share information with a foreign government trusted

traveler program, DHS/CBP is also retaining other foreign governments'

decisions either to approve or deny an application, pursuant to the

applicable joint statements.

 The authority for GES derives from CBP's mandate to secure the

borders of the United States, and to facilitate legitimate trade and

travel. The statutes that permit and define GES include:

 Section 7208 of the Intelligence Reform and Terrorism

Prevention Act of 2004 (IRTPA), as amended, 8 U.S.C. 1365b(k);

 Section 215 of the Immigration and Nationality Act, as

amended, 8 U.S.C. 1185;

 Section 402 of the Homeland Security Act of 2002, as

amended, 6 U.S.C. 202;

 Section 404 of the Enhanced Border Security and Visa

Reform Act of 2002, 8 U.S.C. 1753; and

 Section 433 of the Tariff Act of 1930, as amended, 19

U.S.C. 1433.

 The Regulations that permit and define GES include Parts 103 and

235 of Title 8 of the Code of Federal Regulations. See, especially, 8

CFR 103.2, 103.7, 103.16, 235.1, 235.2, 235.7, and 235.12. Pursuant to

the Independent Offices Appropriations Act of 1952, 31 U.S.C. 9701,

individuals seeking to enroll in trusted traveler or registered

traveler programs must pay a fee when they apply or renew their

membership. See 8 CFR 103.7(b)(1)(ii)(M).

 The purposes of GES have been simplified to reflect that this

system collects information, in advance, from recurring travelers so

that DHS and CBP can assess applicants' eligibility for enrollment in a

GES-supported trusted traveler and registered traveler programs.

 DHS changed the order of routine uses to be consistent with its

practice across all DHS SORNs and for ease of use by DHS personnel.

This change affects the following uses, which were not substantially

changed: Former routine use A is now routine use I;

[[Page 3443]]

former routine use B is now routine use G; former routine use C is now

routine use B; former routine use D is now routine use C; former

routine use E is now routine use A; and former routine use G is now

routine use D.

 This SORN update includes the following substantive changes to

routine uses: In routine use F, the sentence has been added,

``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.'' In routine use G,

reference to ``organizations that are lawfully engaged in collecting

intelligence [\* \* \*] to carry out intelligence responsibilities'' has

been removed because of redundancy. Routine use H has been added to

provide additional transparency on the sharing with foreign governments

for trusted traveler programs and only at the behest of the individual.

Routine use L has been added to allow the Department to share

information with the public when the interests of the public outweigh

those of the individual and only after approval by the DHS Chief

Privacy Officer in consultation with counsel.

 Sharing GES information with partnering foreign countries is

consistent with the routine uses proposed in this System of Records

Notice (SORN), which allows for disclosure to foreign government

agencies to elicit information necessary to make decisions on

applications. Pursuant to CBP's reciprocal joint statements, CBP will

share biographic GE application data and vetting results in the form of

a ``pass/fail'' transmission of U.S. citizens with these foreign

governments only upon receiving the same type of data from those

governments on their citizens who are applying for expedited processing

into the United States. Because of these international information

sharing relationships, CBP is able to make well-informed decisions on

GE applications of citizens from a growing number of countries.

 The retrievability section has been updated to reflect that records

may be retrieved by any of the personal identifiers listed in the

categories of records.

 The retention and disposal section has been updated to reflect that

all GES data is retained for the duration of an individual's active

membership plus three years after an individual's membership is no

longer active, either as a result of expiration without renewal at the

end of a five-year term, as a result of abandonment, or as a result of

CBP termination.

 The notification procedures section has been updated to provide

notice that individuals may view and edit their information through

their online accounts, as well as through the standard procedures under

the Freedom of Information Act and Privacy Act.

 The record source categories have been updated to clarify the

records obtained from the individual and background checks of external

law enforcement systems, as well as providing notice that GES collects

from membership determinations about trusted traveler applicants from

partnering foreign countries.

 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.

 Consistent with DHS' information sharing mission, information

stored in GES may be shared with other DHS components whose personnel

have a need to know the information to carry out their national

security, law enforcement, immigration, intelligence, or other homeland

security functions. In addition, information may be shared 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.

 DHS/CBP is simultaneously issuing a notice of proposed rulemaking

to exempt portions of the DHS/CBP--002 GES SORN from the Privacy Act

requirements. Pursuant to 5 U.S.C. 552a(j)(2) of the Privacy Act, 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, 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)(4)(I), (e)(5) and (e)(8); (f); and (g)(1).

Pursuant to 5 U.S.C. 552a(k)(2), records created during the background

check and vetting process are exempt 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 that this

notice delineates.

 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 routine uses

identified in the GES SORN. The Privacy Act requires that 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, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), DHS 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. This

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 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.

 Below is the description of the DHS/CBP--002 Global Enrollment

System (GES).

 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. Customs and Border

Protection (CBP)--002.

[[Page 3444]]

System name:

 DHS DHS/CBP--002 Global Enrollment System (GES).

Security classification:

 Unclassified, Sensitive, For Official Use Only, Law Enforcement-

Sensitive.

System location:

 Records are maintained at the CBP Headquarters in Washington, DC

and field offices and maintained IT system named the Global Enrollment

Systems.

Categories of individuals covered by the system:

 Individuals who apply to use any form of automated or other

expedited inspection for verifying eligibility to cross the border into

the United States.

Categories of records in the system:

 GES collects the following information on trusted travelers:

 Biographic application data, including:

 Full name;

 Alias(es);

 Date of birth;

 Place of birth;

 Language preference;

 Gender;

 Current and former addresses;

 Telephone numbers;

 Country of citizenship;

 Alien registration number (if applicable);

 Employment history (if available);

 PASS ID or Trusted Traveler membership number;

 Countries visited in the last five years;

 Criminal history (provided by applicant);

 Parental or Legal Guardian permission (if 18 years or

younger);

 Driver's license number;

 Issuing state or province of the applicant's Driver's

License;

 Global Online Enrollment System (GOES) user name and

password (password is maintained in an encrypted format); and

 Answers to security questions to reset password.

 Vehicle or Vessel information, as appropriate, including:

 Flag and home port (where the vessel is foreign flagged);

 Name, registration number, and registration issuing state

or province of the applicant's vessel;

 Make and model, year, color, VIN number, and license plate

number of the vehicle; and

 Owner name, gender, and date of birth.

 Biometric data, including:

 Fingerprints (collected and stored through DHS/USVISIT-

0012 DHS Automated Biometric Identification System (IDENT) for future

identity verification);

 Fingerprint Identification Number (FIN);

 Height;

 Eye color; and

 Facial photographs.

 Information added by DHS/CBP:

 Pointer information to other law enforcement databases

that support the DHS/CBP membership decision;

 Law Enforcement risk assessment worksheet;

 [Pay.gov](http://www.gpo.gov/fdsys/pkg/FR-2013-01-16/html/Pay.gov) tracking number;

 GE membership decision in the form of a ``pass/fail;'' and

 Foreign government membership decisions in the form of a

``pass/fail.''

 The following information is collected on SVRS registered

travelers:

 Full name;

 Gender;

 Date of birth;

 Place of birth;

 Country of citizenship;

 Address;

 Contact telephone number;

 Alternate telephone number;

 Contact email address;

 Password;

 Document type & number (e.g. U.S. Passport, Permanent

Resident Card, Birth Certificate, etc.), place of issue, and expiration

date of document; and

 Vessel information including registration number, hull ID

number, decal number, registered name, location where vessel is

registered, and vessel description (e.g., length, type, manufacturer,

model, year, hull colors, etc.).

 The following information is collected about DTOPS registered

travelers:

 Account name;

 Physical address;

 Shipping address;

 [Pay.gov](http://www.gpo.gov/fdsys/pkg/FR-2013-01-16/html/Pay.gov) tracking number;

 FAST ID, if the conveyance's owner is C-TPAT/FAST

approved;

 Conveyance model year;

 Conveyance manufacturer name;

 Conveyance identification numbers and information, which

are specific to the type of conveyance (e.g., local registration

number, an aircraft's tail number, Coast Guard ID number, vessel name);

 Contact name;

 Contact telephone number; and

 Contact email address.

Authority for Maintenance of the System:

 Section 7208 of the Intelligence Reform and Terrorism Prevention

Act of 2004 (IRTPA), as amended, 8 U.S.C. 1365b(k); Section 215 of the

Immigration and Nationality Act, as amended, 8 U.S.C. 1185; Section 402

of the Homeland Security Act of 2002, as amended, 6 U.S.C. 202; Section

404 of the Enhanced Border Security and Visa Reform Act of 2002, 8

U.S.C. 1753; and Section 433 of the Tariff Act of 1930, as amended, 19

U.S.C. 1433; 31 U.S.C. 9701; Parts 103 and 235 of Title 8 of the Code

of Federal Regulations (See, especially, 8 CFR 103.2, 103.7, 103.16,

235.1, 235.2, 235.7, and 235.12).

Purpose(s):

 The purpose of this system is to assess on an ongoing basis

applicants' eligibility for enrollment in DHS/CBP GES-supported trusted

traveler and/or registered traveler programs.

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 Department of Justice (DOJ), including U.S. Attorney

Offices, or other federal agency conducting litigation or in

proceedings before any court, adjudicative or administrative body, when

it 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 where 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 the National Archives and Records Administration (NARA) or

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;

[[Page 3445]]

 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' 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 an appropriate federal, state, tribal, local, international,

or foreign law enforcement agency or other appropriate authority

charged with investigating or prosecuting a violation or enforcing or

implementing a law, rule, regulation, or order, where a record, either

on its face or in conjunction with other information, indicates a

violation or potential violation of law, 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 foreign governments, at the request of the individual, for

the purpose of applying to that country's trusted traveler program.

 I. To an appropriate federal, state, tribal, local, international,

or foreign law enforcement agency for the purpose of determining an

individual's eligibility for membership in a trusted traveler or

registered traveler program.

 J. To federal and foreign government intelligence or

counterterrorism agencies or components where DHS becomes aware of an

indication of a threat or potential threat to national or international

security, or to assist in anti-terrorism efforts.

 K. To an organization or person in either the public or private

sector, either foreign or domestic, where there is a reason to believe

that the recipient is or could become the target of a particular

terrorist activity or conspiracy, or where the information is relevant

to the protection of life, property, or other vital interests of a

person.

 L. 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 or when

disclosure is necessary to preserve confidence in the integrity of DHS

or is necessary to demonstrate the accountability of DHS' officers,

employees, or individuals covered by the system, except to the extent

it is determined 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:

 Records in this system are stored 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:

 Records may be retrieved by any of the personal identifiers listed

in the categories of records above.

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 permissions.

Retention and disposal:

 CBP is proposing to NARA the following retention: All GES data is

retained for the duration of an individual's active membership plus

three years after an individual's membership is no longer active,

either as a result of expiration without renewal at the end of a five

year term, as a result of abandonment, or as a result of CBP

termination.

System Manager and address:

 Trusted Traveler Program Manager, Office of Field Operations, U.S.

Customs and Border Protection, and Director, Passenger Systems Program

Office, Office of Information and Technology, 1300 Pennsylvania Ave.

NW., Washington, DC 20229.

Notification procedure:

 Individuals may gain access to information on themselves in GES by

directly logging into GOES. Certain information may be amended directly

in the system by the individual such as contact information; however,

other information that was used to determine eligibility, such as date

of birth or gender, may not be changed without contacting DHS/CBP

directly. The Secretary of Homeland Security has exempted portions of

this system from the notification, access, and amendment procedures of

the Privacy Act because it is a law enforcement system. However, DHS/

CBP will consider individual requests to determine whether or not

information may be released. Thus, 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 the

Headquarters or CBP FOIA 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 SW., Building 410,

STOP-0655, Washington, DC 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;

[[Page 3446]]

 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;

and

 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:

 See ``Notification procedure'' above.

Record source categories:

 Records in GES are obtained from the individual and from external

law enforcement systems. The main database checked during the vetting

process, before individuals will be enrolled in any trusted traveler

program, is TECS, which contains historical and enforcement data on

travelers, and provides a gateway to other sources of data. These other

sources include the Terrorist Screening Database, FBI criminal history,

and National Crime and Information Center outstanding wants/warrants,

vehicle and driver's license-related data contained in the

International Justice and Public Safety Network's Nlets system, and

Department of State alien records, lookouts, and status indicators.

Vetting results are also based on checks of the FBI's Integrated

Automated Fingerprint Identification System for criminal history and

IDENT for immigration related records. Trusted traveler applicants from

partnering foreign countries will have membership determinations in GES

from their home country's government.

Exemptions claimed for the system:

 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 that this notice delineates.

 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 routine uses

identified in the GES 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, pursuant to 5 U.S.C. 552a (j)(2) and (k)(2), DHS

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.

 Dated: December 31, 2012.

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2013-00804 Filed 1-15-13; 8:45 am]

BILLING CODE 9111-14-P