[Federal Register Volume 78, Number 49 (Wednesday, March 13, 2013)]
[Notices]
[Pages 15962-15968]
From the Federal Register Online via the Government Printing Office
[www.gpo.gov]
[FR Doc No: 2013-05674]

==========

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0073]

Privacy Act of 1974; Department of Homeland Security, U.S. Customs and Border Protection--DHS/CBP-018--Customs--Trade Partnership Against Terrorism (C-TPAT) System, System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to

[[Page 15963]]

establish a new system of records titled, ``Department of Homeland Security, U.S. Customs and Border Protection, DHS/CBP-018 Customs--Trade Partnership Against Terrorism System of Records.'' This system of records allows the Department of Homeland Security/U.S. Customs and Border Protection, DHS/CBP-018, Customs-Trade Partnership Against Terrorism to collect and maintain records about members of the trade community related to Customs and Border Protection's Customs-Trade Partnership Against Terrorism program. Businesses accepted into the program, called partners, agree to analyze, measure, monitor, report, and enhance their supply chains in exchange for greater security and facilitated processing offered by Customs and Border Protection. The Customs-Trade Partnership Against Terrorism program allows Customs and Border Protection to focus its resources on higher risk businesses and thereby assists the agency in achieving its mission to secure the border and facilitate the movement of legitimate international trade. This new system of records collects and manages information, including personally identifiable information, about prospective, ineligible, current, or former trade partners in Customs-Trade Partnership Against Terrorism, and other entities and individuals in their supply chains. This system also collects and maintains information, including personally identifiable information, regarding members of a foreign government secure supply chain program that have been recognized by Customs and Border Protection, through a mutual recognition arrangement or comparable arrangement, as being compatible with the program. The

Customs-Trade Partnership Against Terrorism program provides a Security Link Portal, which allows partners and applicants to access and manage their information. Customs and Border Protection is publishing this new system of records notice in order to notify the public about the system, permit trade partners access to the information they provide, and offer a description of how and where information is collected and maintained. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking elsewhere in the Federal Register, to exempt this system of records from certain provisions of the Privacy Act. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: The new system of records will be effective April 12, 2013, unless comments are received that result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0073 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 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.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-325-0280), CBP Privacy Officer, U.S. Customs and Border Protection, 90 K Street NE. 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), US Customs and Border Protection (CBP) proposes to establish a new DHS system of records titled, ``DHS/CBP-018-C-TPAT System of Records.''

CBP is publishing this new system of records notice to notify the public about the system and offer a description of how CBP collects and maintains information pertaining to prospective, ineligible, current, or former trade partners in C-TPAT; other entities and individuals in their supply chains; and members of foreign governments' secure supply chain programs that have been recognized by CBP, through a mutual recognition arrangement or comparable arrangement, as being compatible with C-TPAT.

CBP will use the information collected and maintained through the C-TPAT program to carry out its trade facilitation, law enforcement, and national security missions. In direct response to 9/11, CBP challenged the trade community to partner with the government to design a new approach to supply chain security--one that protects the United

States from acts of terrorism by improving security while facilitating the flow of compliant cargo and conveyances. The result was the Customs-Trade Partnership Against Terrorism (C-TPAT)--an innovative, voluntary government/private sector partnership program. C-TPAT is a voluntary program in which certain types of businesses agree to cooperate with CBP in the analysis, measurement, monitoring, reporting, and enhancement of their supply chains.

Businesses accepted in to C-TPAT are called partners and agree to take actions to protect their supply chain, identify security gaps, and implement specific security measures and best practices in return for facilitated processing of their shipments by CBP. The program focuses on improving security from the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination. The current security guidelines for C-TPAT program members address a broad range of topics including personnel, physical and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing. These guidelines offer a customized solution for the members, while providing a clear minimum standard that approved companies must meet.

Businesses eligible to fully participate in C-TPAT include U.S. importers; U.S./Canada highway carriers; U.S./Mexico highway carriers; rail and sea carriers; licensed U.S. Customs brokers; U.S. marine port authority/terminal operators; U.S. freight consolidators; ocean transportation intermediaries and non-operating common carriers; Mexican and Canadian manufacturers; and Mexican long-haul carriers. As part of its development, CBP plans to include exporters from the United States in C-TPAT.

There are three tiers of C-TPAT partnership, with each tier having its own set of requirements and corresponding facilitated processing. In general, businesses are considered applicants until CBP has vetted the information in the application and accepted the business into the program. Once accepted, the business is designated as a Tier One certified partner, and a site visit is arranged. The site visit is used to validate the partner's supply chain security and leads to importers becoming Tier Two validated partners. As C-TPAT has incorporated other eligible business types, it has led

to those businesses becoming certified, validated non-importers. If an importer with Tier Two validated partner status exemplifies best practices in its supply chain security, it may attain Tier Three validated partner status. As a business progresses up the tiers, it receives more facilitated processing at ports of entry.

Information is collected directly from C-TPAT partners or applicant businesses seeking membership in C-TPAT and indirectly from trade partners or through Mutual Recognition Arrangements (MRA) or memoranda of understanding relating to harmonization efforts between CBP and the foreign secured supply chain program. In the course of enrolling, certifying, and validating C-TPAT trade partners and their supply chains, the C-TPAT system will receive personally identifiable information (PII) and confidential business information from trade entities and their representatives.

To participate in the C-TPAT program, a company is required to submit a confidential, on-line application using the C-TPAT Security Link Portal, https://ctpat.cbp.dhs.gov. The C-TPAT Security Link Portal

is the public-facing portion of the C-TPAT system used by applicants to submit the information in their company and supply chain security profiles. Initially, the applicant business provides basic business-identifying information in the company profile using the online application form. This business-identifying information is used to verify the identity and actual existence of the applicant business and may include basic identifying elements and/or PII used in the importation of cargo, such as U.S. Social Security Numbers (SSN) for sole proprietors, Internal Revenue Service Business Identification Numbers, and Customs assigned identification numbers (such as Manufacturer Identification numbers and Broker/Filer codes, etc.). Point of contact information is collected for the business, as well as owner information.

Additionally, the applicant business must complete a Supply Chain Security Profile (SCSP). The information provided in the SCSP is a narrative description of the procedures the applicant business uses to adhere to each C-TPAT Security Criteria or Guideline articulated for their particular business type (importer, customs broker, freight forwarder, air, sea, and land carriers, contract logistics providers, etc.) together with any supporting documentation. Data elements entered by the applicant business are accessible for update or revision through the C-TPAT Security Link Portal. An applicant's SCSP must provide supply chain security procedures for each business in the applicant's supply chain, even if those businesses are not, or do not desire to become partners of C-TPAT separately. This information is focused on the security procedures of those businesses (e.g., whether the business conducts background investigations on employees), rather than the individuals related to those businesses (e.g., a list of employee names).

A CBP Supply Chain Security Specialist (SCSS) vets the SCSP information provided by the applicant by querying that information through various information sources and systems, and queries of publicly available data (e.g., through Google). The SCSS will then evaluate the SCSP information against the results provided by such system vetting, derogatory or otherwise, and indicate whether the applicant is fit for the program in the Security Link Portal. Derogatory vetting results are incorporated into an issue paper for a C-TPAT supervisor's approval, and the issue paper is stored separately from the Security Link Portal on an internal C-TPAT SharePoint, which is only accessible by appropriate CBP employees and supervisors.

Vetting results containing PII are not stored in the C-TPAT Security Link Portal. When a query reveals derogatory information about a business applicant or partner, the SCSS makes a notation on the internal portion of the C-TPAT Security Link Portal indicating the existence of derogatory information and a citation to the appropriate records. For instance, if a query of an applicant in TECS results in derogatory information, the TECS ID is used as an identifier for the record in the C-TPAT Security Link Portal, rather than the contents of the TECS record. However, specific details regarding the incident or violation giving rise to the unfavorable analysis will be maintained within the C-TPAT SharePoint site and the relevant source system. The SCSS is responsible for vetting all C-TPAT applicants, and conducts this vetting of business entities every 6-12 months to ensure continued compliance.

Consistent with DHS's information sharing mission, information stored in DHS/CBP-018 Customs--Trade Partnership Against Terrorism (C-TPAT) System may be shared with other DHS components that 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.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This newly established 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 for 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 where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/CBP-018 Customs--Trade Partnership Against Terrorism (C-TPAT) System of Records. 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)-018.

System name:

DHS/CBP-018 Customs--Trade Partnership Against Terrorism (C-TPAT)

Security classification:

Unclassified, for official use only, law enforcement sensitive.

System location:

Records are maintained at CBP Headquarters, Washington, DC and field offices in C-TPAT's Security Link Portal and a CBP collaborative intranet.

Categories of individuals covered by the system:

Individuals, including Points of Contact (POC), owners, and others associated with prospective, ineligible, current, or former C-TPAT business

entities; individuals associated with the supply chain of such C-TPAT business entities; and individuals associated with business entities in foreign governments secure supply chain programs that have been recognized by CBP, through harmonization, a mutual recognition

arrangement, or comparable arrangement, as being compatible with C-TPAT.

Categories of records in the system:

At the Application level, information is collected from the applicant about itself and those members of its international supply chain. Pre-set fields of business-identifying information within the company profile portion of the online application include:

- Business Entity Type;
- Application Exception Token;
- Legal Business Name;
- Other Name(s) by which the Business is known (i.e., ``Doing Business As''), if applicable;
- Business Telephone;
- Business Fax;
- Business Web site address;
- Business history;
- Physical Address(es);
- Mailing Address(es);
- Owner Type: (e.g., Corporation\ Partnership\Sole Proprietor, etc.);
- Years in Business;
- Number of Employees;
- Business Points of Contacts;
- First Name;
- Last Name;
- Title;
- Email Address (also used to log in to the Security Link Portal);
- Password;
- Telephone Number;
- Contact Type;
- U.S. Social Security Numbers (as volunteered by sole proprietors as their tax identification number);
- Internal Revenue Service Business Identification Numbers;
- Customs assigned identification numbers (Importers of Record (IOR) number; Manufacturer Identification Numbers (MID) and Broker/Filer codes, etc.);
- Issue Papers, including information regarding whether the applicant is eligible for C-TPAT membership or source record numbers for such information;
- Narrative description of supply chain security procedures for applicant and other entities in applicant's supply chain;
- Validation supporting documentation (e.g., bills of lading; audits--internal & external; proof of background checks; contractual obligations; via a letter from a senior business partner officer attesting to compliance; statements demonstrating compliance with C-TPAT security criteria or an equivalent World Customs Organization accredited security program administered by a foreign customs authority; importer security questionnaire); and
- Account Status.

Information received from and confirmed to countries with which CBP has a Mutual Recognition Arrangement (MRA) includes:

- Legal Business Name;
- Other Name(s) by which the Business is known (i.e., ``Doing Business As''), if applicable;
- Company Type;

Date Partner Certified;
Account Status;
Vetting Status;
Date Validation Completed;
SCSS Name;
Office Assigned Name;
Mutual Recognition Country;
Business identifying numbers, e.g.:
[cir] Standard Carrier Alpha Code (SCAC);
[cir] IOR;
[cir] MID;
By Applicant request, information received from, and forwarded to, foreign secure supply chain programs pursuant to a harmonization program may include, but is not limited to:
Legal Name;
Doing Business As;
Telephone Number;
Fax Number;
Web site;
Owner Type;
Business Start Date;
Number of Employees;
Brief Company History;
Primary Address, Type;
Primary Address, Name;
Primary Address, Country;
Primary Address, Street Address;
Primary Address, City;
Primary Address, State/Province;
Primary Address, Zip/Postal Code;
Mailing Address:
[cir] Type;
[cir] Name;
[cir] Country;
[cir] Street Address;
[cir] City;
[cir] State/Province; and
[cir] Zip/Postal Code.
Primary Contact:
[cir] Email Address;
[cir] Type;
[cir] Salutation;
[cir] First Name;
[cir] Last Name;
[cir] Title; and
[cir] Telephone Number.
Partner Notifications;
Number of Entries;
U.S. Department of Transportation (DOT) Issued Number;
U.S. National Motor Freight Traffic Association Issued;
SCAC;
Dun & Bradstreet Number;
Services Offered;
Driver Sources;
Entries related to harmonization country;
The entire Security Profile (Upon Request):
[cir] Account Number;

[cir] Risking Status;
[cir] MSR Status;
[cir] Validation Type;
[cir] Validation Closed Date;
[cir] Validation Status;
[cir] Validation Type Verification (Government Contact);
[cir] Verification Type Start Date;
[cir] Verification Type: (phone, visit, mutual recognition);
[cir] Verification Visit address;
[cir] Business Type; and
[cir] Harmonization Host Program.
Account Status;
Vetting Status;
Minimum Security Requirements/Security Profile Status;
Validation Status; and
Harmonization Status.

Authority for maintenance of the system:
This system and program are authorized by 6 U.S.C. 901 note (Security and Accountability for Every Port Act of 2006 (SAFE Port Act), including 6 U.S.C. 961-973. Pilot programs enhancing secure supply chain practices related to C-TPAT are also authorized by Homeland Security Presidential Directive/HSPD-8, ``National Preparedness'' Section 22 (December 17, 2003).

Purpose(s):
The purpose of this system is to verify the identity of C-TPAT partners, determine enrollment level, and provide identifiable ``low risk'' entities with fewer random checks and facilitated processing. The information will be cross-referenced with data maintained in CBP's other cargo and enforcement databases and will be shared with other law enforcement systems, agencies or foreign entities, as appropriate, when related to ongoing investigations or operations. Information will be used to analyze, measure, monitor, report, and enhance business supply chains to permit facilitated processing of C-TPAT partner shipments by CBP.

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.

[[Page 15966]]

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). Any disclosure of information must be made consistent with the official duties of the person making the disclosure. The routine uses are as follows:
A. To the Department of Justice (DOJ), including the United States Attorneys 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 of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity when 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;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individuals 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's 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, when 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.

H. To appropriate foreign governmental agencies or multilateral governmental organizations pursuant to an arrangement between CBP and a foreign government or multilateral governmental organization regarding supply chain security.

I. To an appropriate federal, state, local, territorial, tribal, or foreign governmental agencies or multilateral governmental organizations or other appropriate authority or entity when necessary to vet a C-TPAT applicant or validate a C-TPAT partner.

J. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be relevant in countering the threat or potential threat.

K. To a federal, state, tribal, or local agency, or other appropriate entity or individual, or foreign governments, in order to provide relevant information related to intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

L. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant and necessary to the protection of life or property.

M. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation.

N. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit.

O. To a federal, state, local, tribal, or foreign governmental agency or multilateral governmental organization for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

P. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital health interests of a data subject or other persons (e.g., to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk).

Q. 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's 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.