9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2012-0073]

Privacy Act of 1974: Implementation of Exemptions; 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, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/ U.S. Customs and Border Protection, DHS/CBP-018- Customs – Trade Partnership Against Terrorism (C-TPAT) 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 [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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, D.C. 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 E. Castelli (202-325-0280), CBP Privacy Officer, U.S. Customs and Border Protection, 90 K Street N.E. 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, D.C. 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) is giving concurrent notice of a newly established system of records for the DHS/CBP-018-C-TPAT System of Records and this proposed rulemaking.

CBP is publishing a 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 (other business types become 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 personally identifiable information (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.

DHS is issuing this Notice of Proposed Rulemaking to exempt portions of the system of records from certain provisions of the Privacy Act.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the U.S. Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. 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 portions of DHS/CBP-018- Customs – Trade Partnership Against Terrorism (C-TPAT) System of Records. Information in DHS/CBP-018- Customs – Trade Partnership Against Terrorism (C-TPAT) System of Records relates to official DHS national security, law enforcement, and intelligence 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; 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.

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-018- Customs – Trade Partnership Against Terrorism (C-TPAT) 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 is revised 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. Add new paragraph 70 at the end of Appendix C to part 5 to read as follows:

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

* * * * *

70. The DHS/CBP-018- Customs – Trade Partnership Against Terrorism (C-TPAT) System of Records consists of electronic and paper records and will be used by

DHS and its components. The DHS/CBP-018- Customs – Trade Partnership Against Terrorism (C-TPAT) System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security activities. The DHS/CBP-018- Customs – Trade Partnership Against Terrorism (C-TPAT) System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. CBP will not assert any exemption with respect to information requested from and provided by the C-TPAT applicant including, but not limited to, company profile, supply chain information and other information provided during the application and validation process. CBP will not assert any exemptions for an individual's application data and final membership determination in response to a request from that individual. However, the Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement agency has sought particular records may affect ongoing law enforcement activities. As such, pursuant to 5 U.S.C. 552a(j)(2), the Secretary of Homeland Security has exempted this system from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information. Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, all other C-TPAT data, including information regarding the possible ineligibility of an

applicant for C-TPAT membership discovered during the vetting process and any resulting issue papers, 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). Pursuant to 5 U.S.C. 552a(k)(2), information regarding the possible ineligibility of an applicant for C-TPAT membership discovered during the vetting process and any resulting issue papers are exempt 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H),(e)(4)(I); and (f). 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.

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

Dated: February 22, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-05673 Filed 03/12/2013 at 8:45 am; Publication Date: 03/13/2013]