The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 1 of 9

PRIVACY THRESHOLD ANALYSIS (PTA)

**This form is used to determine whether
a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSOnline and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 2 of 9

PRIVACY THRESHOLD ANALYSIS (PTA)

Please complete this form and send it to the DHS Privacy Office.
Upon receipt, the DHS Privacy Office will review this form
and may request additional information.

SUMMARY INFORMATION

DATE submitted for review: June 23, 2009

NAME of Project: Customs Trade Partnership Against Terrorism (C-TPAT)

Name of Component: Customs and Border Protection

Name of Project Manager: Lamont Newton

Email for Project Manager: LAMONT.NEWTON@DHS.GOV

Phone number for Project Manager: 703-553-1785

TYPE of Project:

☒ **Information Technology and/or System***

☐ **A Notice of Proposed Rule Making or a Final Rule.**

☐ **Other: <Please describe the type of project including paper based Privacy Act system of records.>**

---

* The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).

- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note, for purposes of this form, there is no distinction made between national security systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 3 of 9

SPECIFIC QUESTIONS

1. **Describe the project and its purpose:**

The objective of Customs Trade Partnership Against Terrorism C-TPAT is to further the efforts of CBP to secure entry of goods into the United States from terrorist infiltration and the introduction of other illegal activities. One of the best means to prevent further terrorist attacks is to use border authorities to make it more difficult for terrorist and terror weapons to enter the U.S. and to better secure the international supply chain by preventing terrorist access to transportation modalities, thereby eliminating the potential for trafficking of implements of terror within the global supply chain. The C-TPAT system is a critical component of reaching that goal, because it provides a mechanism to meet the C-TPAT mandate: to inform and engage its members in a way that will continue to foster and improve global supply-chain security. This goal directly supports the Department of Homeland Security (DHS) efforts to secure supply channels by enlisting Trade Partners in security efforts.

C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. C-TPAT offers trade-related businesses an opportunity to play an active role in the war against terrorism. By participating in this first worldwide supply chain security initiative, companies will ensure a more secure and expeditious supply chain for their employees, suppliers and customers. To participate, businesses must apply online at https://ctpat.cbp.dhs.gov/CompanyProfile.aspx , through a CBP host site.

The PIA was submitted to the CBP Privacy Office in May 2008 and is currently awaiting review and approval.

2. **Status of Project:**

☐ This is a new development effort.

☒ This is an existing project.

Date first developed: March 1, 2006

Date last updated: May 1, 2009

<Please provide a general description of the update.>

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 4 of 9

3.   **Could the project relate in any way to an individual?[1]**

☐ No. Please skip ahead to the next question.

☒ Yes. Please provide a general description, below.

Initially, business-identifying information is collected by C-TPAT through the online application form. Business-identifying information may include identification numbers such as U.S. Social Security Numbers for sole proprietors, Internal Revenue Service Business Identification Numbers, Customs assigned identification numbers such as Manufacturer Identification numbers and Broker/Filer codes, etc.

Pre-set fields of business-identifying information within the online application include:

Business Entity Type

Tax Identification Number (TIN)

Legal Company Name

Company "Doing Business As"

Company Telephone

Company Fax

Physical Address

Mailing Address

Owner Type: (Select) Corporation\ Partnership\ Sole Proprietor

Years In Business

Number of Employees

Company Contacts

First Name

Last Name

Title

Email Address

Telephone

---

[1] Projects can relate to individuals in a number of ways. For example, a project may include a camera for the purpose of watching a physical location. Individuals may walk past the camera and images of those individuals may be recorded. Projects could also relate to individuals in more subtle ways. For example, a project that is focused on detecting radioactivity levels may be sensitive enough to detect whether an individual received chemotherapy.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 5 of 9

Contact Type

4. **Do you collect, process, or retain information on: (Please check all that apply)**

☐ DHS Employees

☐ Contractors working on behalf of DHS

☒ The Public

☐ The System does not contain any such information.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

5. **Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)**

☒ No.

☐ Yes. Why does the program collect SSNs? Provide the function of the SSN and the legal authority to do so:

6. **What information about individuals could be collected, generated or retained?**

> Tax Identification Number (TIN)
>
> Legal Company Name
>
> Company "Doing Business As"
>
> Company Telephone
>
> Company Fax
>
> Physical Address
>
> Mailing Address
>
> Company Contacts
>
> First Name
>
> Last Name
>
> Title
>
> Email Address
>
> Telephone

7. **If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?**

☒ No. Please continue to the next question.

☐ Yes. Is there a log kept of communication traffic?

> ☒ No. Please continue to the next question.
>
> ☐ Yes. What type of data is recorded in the log? (Please choose all that apply.)
>
> > ☐ Header

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 7 of 9

☐ Payload Please describe the data that is logged.

<Please list the data elements in the log.>

8. **Can the system be accessed remotely?**

    ☐ No.

    ☒ Yes.   When remote access is allowed, is the access accomplished by a virtual private network (VPN)?

    > ☒ No. C-TPAT is an outward facing system that is only accessible via the internet for both internal and external users. The connection (session) is encrypted via HTTPS over TLS and the certificates are generated from DHS.

    > ☐ Yes.

9. **Is Personally Identifiable Information[2] physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)**

    ☐ No.

    ☒ Yes. Trade Partners are only able to access their own information, therefore any removal of such PII informtiaon is limited to what pertains to them.

10. **Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[3]?**

    ☒ No

    ☐ Yes. Please list:

11. **Are there regular (ie. periodic, recurring, etc.) data extractions from the system?**

    ☐ No.

---

[2] Personally Identifiable Information is information that can identify a person. This includes; name, address, phone number, social security number, as well as health information or a physical description.

[3] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in TAFISMA.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 8 of 9

☒ Yes. Are these extractions included as part of the Certification and Accreditation[4]?

    ☒ Yes.

    ☐ No.

12.   **Is there a Certification & Accreditation record within OCIO's FISMA tracking system?**

☐ Unknown.

☐ No.

☒ Yes. Please indicate the determinations for each of the following:

Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

---

[4] This could include the Standard Operation Procedures (SOP) or a Memorandum of Understanding (MOU)

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 9 of 9

PRIVACY THRESHOLD REVIEW

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: October 22, 2009

NAME of the DHS Privacy Office Reviewer: Rebecca J. Richards

DESIGNATION

☐ **This is NOT a Privacy Sensitive System** – the system contains no Personally Identifiable Information.

☒ **This IS a Privacy Sensitive System**
   Category of System
   ☒ IT System

   ☐ National Security System

   ☐ Legacy System

   ☐ HR System

   ☐ Rule

   ☐ Other:

   Determination
   ☐ PTA sufficient at this time

   ☐ Privacy compliance documentation determination in progress

   ☐ PIA is not required at this time

   ☒ A PIA is required

      ☐ System covered by existing PIA:

      ☒ A new PIA is required.

      ☐ A PIA Update is required.

   ☒ A SORN is required

      ☐ System covered by existing SORN:

      ☒ A new SORN is required.

DHS PRIVACY OFFICE COMMENTS