Privacy Impact Assessment
for the

Customs-Trade Partnership Against Terrorism (C-TPAT)

February 14, 2013

DHS/CBP/PIA-013

Contact Point
Shawn Beddows
Acting Director, C-TPAT
U.S. Customs and Border Protection
(202) 344-2619

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Customs-Trade Partnership Against Terrorism (C-TPAT), is a U.S. Customs and Border Protection (CBP) voluntary trade partnership program in which CBP and members of the trade community work together to secure and facilitate the movement of legitimate international trade. The program focuses on improving security throughout the supply chain, beginning at the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination. C-TPAT member companies, called partners, agree to implement certain security procedures throughout their supply chains to protect those supply chains from terrorist infiltration and other illegal activities that threaten the security of the United States. C-TPAT partners who undertake these protections receive facilitated processing by CBP. As a result, the program helps CBP achieve its twin goals of improving security while facilitating the flow of global trade. In the course of enrolling, certifying, and validating C-TPAT applicants/partners and their supply chains, the C-TPAT system will receive personally identifiable information (PII) and confidential business information from the applicant/partner, as well as sensitive law enforcement information from existing law enforcement systems.

Overview

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 government/private sector partnership program.[1] 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.

C-TPAT is a supply chain security program for international cargo and conveyances. It increases security measures, practices, and procedures throughout all sectors of the international supply chain. Central to the security vision of C-TPAT is the core principle of increased facilitation for legitimate business entities that are compliant traders. All C-TPAT benefits are privileges offered to only the most secure and compliant program participants.

C-TPAT builds on the best practices of CBP/industry partnerships to strengthen supply chain security, encourage cooperative relationships, and better concentrate CBP resources on areas of greatest risk. This partnership between CBP and the trade industry is built on CBP's border authority and cooperative relationships. To uphold this relationship, accountability is required. The trade partner must be willing to assume responsibility for securing its supply chain according to agreed-upon security standards and implementing changes as needs arise.

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

[1] On Oct. 13, 2006, the President signed the Security and Accountability For Every Port Act of 2006 (SAFE Port Act), 6 U.S.C. § 901 note, which legislatively authorized the establishment of CBP's Customs-Trade Partnership Against Terrorism program (C-TPAT).

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[2], validated[3] 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. The process is described in greater detail below.

Application

To participate in the C-TPAT program, a company must 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 personally identifiable information (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

[2] A certified business is one that C-TPAT has vetted and accepted its supply chain security chain profile.
[3] A validated entity is a certified business whose supply chain security has received a joint evaluation by a Supply Chain Security Specialist (SCSS) and the C-TPAT partner.

(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.[4] 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).

Applicant Vetting

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, including, but not limited to, TECS,[5] the Automated Commercial System (ACS),[6] the Automated Commercial Environment (ACE),[7] the Automated Targeting System (ATS),[8] 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.[9]

Tier One Certified Partners

Once CBP has vetted an applicant's supply chain security profile and accepts the applicant into the C-TPAT program, the applicant is reclassified as a "certified" partner and immediately begins to receive facilitated processing. Such facilitation includes appropriate adjustments to the partner's risk

[4] See the links in Appendix C for a visual explanation of the application process.
[5] SORN at 73 Fed. Reg. 77,778 (December 19, 2008).
[6] SORN at 73 Fed. Reg. 77,759 (December 19, 2008). PIA available online at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_acs10plus2.pdf
[7] SORN at 71 Fed. Reg. 3109 (January 19, 2006).
[8] SORN at 72 Fed. Reg. 43,567 (August 6, 2007). PIA available online at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate10plus2.pdf
[9] Highway carriers participating in CBP's Free and Secure Trade (FAST) program are initially vetted through FAST and then re-vetted and certified by C-TPAT.

assessment, expedited cargo processing at the border (including access to certain lanes for highway carriers on the Canadian and Mexican borders), eligibility for the Importer Self-Assessment Program, participation in C-TPAT supply chain security seminars, and an assigned SCSS to serve as a liaison between the partner and CBP. An internal Status Verification Interface (SVI) function allows partners to view each other's C-TPAT status. Participation in this function is voluntary; partners can opt-in by generating and sharing an SVI number with other users, which makes their status visible to other users. Partners can opt-out by generating a new SVI number to distribute, which invalidates the previous SVI number. Participating partners also have access to instant messaging with the assigned SCSS, access to uploaded SCSS reports, and published C-TPAT documents.

Tier Two Validated Partners and Certified, Validated Non-Importers

One the applicant has become a certified partner in C-TPAT, CBP schedules the certified partner for a validation review. The validation process allows importers to become Tier Two validated partners. Other certified partners that are not importers may go through the validation process to become certified, validated non-importers. The purpose of a validation review is for CBP to verify that the security profile submitted by the partner is accurate, and that its supply chain is in compliance with C-TPAT minimum security criteria. In addition to the facilitated processing granted to Tier One certified partners, Tier Two validated partners receive a lower likelihood of cargo examinations than those received by Tier One partners. In addition, Tier Two partners are eligible for priority searches of cargo, meaning "front-of-the-line" inspection privileges at ports of entry, should an examination be required.

During validation of an Importer, SCSSs verify supply chain security processes and procedures. SCSSs inspect both domestic and foreign sites of a partner's supply chain through on-site visits. A validation review is not an independent audit, but a joint evaluation of the partner's supply chain by the SCSS and the C-TPAT partner. The SCSS generally gives the partner at least 30 days written notice prior to the validation review. Additionally, the SCSS and the partner jointly decide on the scope of the validation review and the inspection areas. During this process, the SCSS may collect further documentation of the partner's supply chain security practices and store them in the partner's C-TPAT profile. For those business entities eligible for C-TPAT certification (carriers, ports, terminals, brokers, consolidators, etc.) in the partner's supply chain, the partner must articulate in the SCSP narratives or uploaded documentation whether these supply chain businesses are C-TPAT certified. They may do this by providing the C-TPAT certificate and/or SVI number for the supply chain business. For those businesses that are not eligible for C-TPAT certification, partners must demonstrate that those businesses are meeting C-TPAT security criteria via written/electronic confirmation[10] and upload those documents into the security profile.

At the conclusion of the validation review, the SCSS writes a report that includes all of the validation review findings and a risk assessment. Partners may not view the risk assessment, but they may access the report describing CBP analysis and assessment of the partner's supply chain security to aid the

[10] For example: contractual obligations; via a letter from a senior business officer attesting to compliance; a written statement from the business demonstrating their compliance with C-TPAT security criteria or an equivalent World Customs Organization accredited security program administered by a foreign customs authority; or, by providing a completed importer security questionnaire.

partner with its certification or validation compliance measures. The C-TPAT partner may access the report through the Partner Document Exchange in the Security Link Portal. If a SCSS identifies security deficiencies during the validation, it may cease certain facilitated processing of the C-TPAT partner, or remove the partner from the program.

Tier Three Partnership Requirement - Meeting Security Best Practices

An importer partner can achieve Tier Three status only if the validation shows the partner exhibits security best practices that exceed the minimum security criteria. Therefore, Tier Three partners must exceed the guidelines established for validation as a Tier Two partner of C-TPAT. CBP will consider any relevant law enforcement or compliance violations on record in determining whether Tier Three status is appropriate. Additionally, the partner must use advanced container security devices and technologies, and supply chain security must be embraced at the highest levels of the company. Tier Three partners receive all of the facilitated processing of Tier One and Tier Two status. They are also eligible to receive further appropriate adjustments to their ATS scores, exceeding those of Tier One and Tier Two partners. In addition, Tier Three partners may receive: (1) further reduction in the likelihood of cargo examinations; (2) highest priority when examinations of cargo are required; (3) inclusion in joint incident management exercises; (4) participation in secure supply chain pilot programs; and (5) permission to use a "Green Lane," which allows the expedited release of cargo in U.S. ports during all threat levels.

Mutual Recognition

CBP has Mutual Recognition Arrangements (MRA) with certain foreign nations with secure supply chain programs that are compatible with C-TPAT (see Appendix B). Businesses that participate in compatible secure supply chain programs, which are identified in MRAs, generally receive facilitated processing comparable to C-TPAT partners. If a foreign partnership program that is recognized in an MRA conducts a validation of a business in its program, the foreign partnership program will send the business' Manufacturer Identification Numbers (MID) to C-TPAT. C-TPAT vets the entities using the MID, which is then uploaded to CBP's ATS for appropriate adjustments to the foreign manufacturer's cargo risk assessment. This process saves CBP the time and resources involved in visiting the foreign company to conduct on-site inspections. Businesses that participate in a partner country program the subject to an MRA do not have a C-TPAT Security Portal Link account (i.e., only C-TPAT partners have a C-TPAT Security Portal Link account).

Harmonization

CBP plans to pursue harmonization with foreign secured supply chain programs, which will allow C-TPAT partners to become members in foreign secured supply chain programs and allow members in foreign secured supply chain programs to become C-TPAT partners. Harmonization allows C-TPAT partners to share their application information and C-TPAT status information located on the C-TPAT Security Link Portal with the foreign secure supply chain program. Harmonization programs similarly allow members of the foreign secure supply chain program to share their application and status information with C-TPAT, and this information would be stored on the C-TPAT Security Link Portal. Additionally, if harmonization is achieved, certain employees of the foreign secure supply chain program will have read-only access to the C-TPAT Security Link Portal to evaluate partners for eligibility in the

foreign supply chain program. Employees of the foreign secure supply chain program with such access would be subject to the same or equivalent requirements as other C-TPAT users. Each program would conduct its own vetting and determine its own eligibility. A list of foreign secure supply chain programs with which CBP has harmonized C-TPAT is provided and will be updated in Appendix B.

Excepted Partnership

Certain entities, including foreign manufacturers from countries with which CBP does not have an MRA, are not eligible to receive facilitated processing under the C-TPAT program, but may still wish to be part of the program. The C-TPAT Director may grant C-TPAT partnership status to an otherwise ineligible entity by issuing an Application Exception Token, which permits them to apply through the Security Link Portal. These interested entities must abide by the same high standards as other partners, but are not granted preferred processing at U.S. ports or other facilitated processing.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

This system and program are authorized by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), 6 U.S.C. § 901 note, as amended. 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).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

C-TPAT is covered under the new C-TPAT SORN (DHS/SORN/CBP-018), and will be published concurrently with this PIA and found at www.dhs.gov/privacy.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. C-TPAT has undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with Federal statutes, policies, and guidelines. The system re-certified its Authority to Operate on May 1, 2012.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. CBP will work with the NARA to develop a retention and disposition schedule for C-TPAT records that will meet program requirements. CBP proposes to purge any non-derogatory information 5 years after the entity exits the program, and 25 years for any derogatory information.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The OMB control number for the C-TPAT Security Link Portal is 1651-0077.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

At the Application level, CBP collects information 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 (e.g., "Doing Business As"), if applicable;
- Business Telephone;
- Business Fax;
- Business website 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.);

- Account Status; and
- 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.)

The SCSS vetting an application may collect and store notes or results from the vetting of the above information in the applicant's C-TPAT profile. Derogatory data extracted from system and background inquiries may be retained in an internal C-TPAT SharePoint as part of the vetting process by the SCSS. Derogatory results from vetting an application are incorporated into an issue paper and stored on an internal C-TPAT SharePoint, which is only accessible by C-TPAT employees and supervisors.

At the Tier Two level, information is provided by the applicant in the supply chain security profile as a narrative description of the procedures the applicant uses to ensure adherence to each C-TPAT Security Criteria or Guideline articulated for their particular business type. Together with any supporting documentation, that narrative is uploaded to the "Documents" section in the C-TPAT Security Link Portal. Examples of the C-TPAT Security Criteria or Guidelines include security processes and procedures for:

- the integrity of the shipment at the point of origin;
- container security, container inspection;
- container seals;
- container storage;
- physical access controls to the partner's locations;
- employee identification, issuance, removal, and changing of devices (keys, badges etc.);
- visitors;
- deliveries;
- challenging and removing an unauthorized individual;
- personnel security;
- pre-employment verification;
- background investigations on prospective employees;
- personnel termination procedures;
- procedural security;
- documentation processing;
- manifesting procedures;
- shipping & receiving;
- cargo discrepancies;
- security training & awareness;
- physical security of the supply chain businesses physical locations including fencing, gates and gate houses, parking building structure, locking and key devices, lighting and alarm/video surveillance systems; and
- information technology security password protection and accountability.

In general, the information in these narrative fields as well as the documents to support the explanation provided will pertain to all of the applicant's supply chain businesses from point of origin (manufacturer/supplier/vendor) through the point of distribution. During the course of providing these narratives, uploading documents, and investigating the applicant's supply chain, a variety of business confidential and personally identifiable information may be collected. However, this information is incidentally collected and always in context of the applicant business.

After an applicant's information is analyzed by an SCSS, applicants are provided an "Account Status," hierarchically categorized by completeness of acceptable security elements. The account status designation is used to identify an entity's status within the C-TPAT program. Account statuses include:

- Pre-Applicant: The business has submitted their company profile, but the system has not received their security profile to complete the application.
- Certified: The business has completed requirements for certification with nothing further requested at this time other than the yearly self-assessment.
- Certified, Exceeding: The business is C-TPAT certified, validated importers that exceed minimum-security criteria.
- Certified, Validated: The business is C-TPAT certified and validated importers. The company meets minimum importer security criteria.
- Certified, Validated Non-importers: The business is not an importer, but has been certified and validated.
- Withdrawn: The business withdrew its application.
- Rejected: The business's security profile has been reviewed and determined that C-TPAT partnership was not appropriate. If this decision was reached because the company's security profile was deficient, the business, at its option, can correct the rejected sections and resubmit the profile for reconsideration.
- Applicant: The business has submitted their online application and it is being processed by C-TPAT. No disposition has been made.
- Validated, Suspended: A business whose facilitated processing has been suspended, for example, due to negative findings during the validation, however the business has demonstrated that it is attempting to rectify the problem.
- Validated, Removed: A business that has been removed from the program, for example, because the business received a negative review on their validation.
- Incident, Suspended: C-TPAT Partner has been suspended due to infraction(s).
- Incident, Removed: C-TPAT Partner has been removed from the program due to infraction(s) (e.g. egregious incident, company involvement, past incidents, etc.).
- Ineligible: The business was found to lack the requirements criteria to be a partner in the C-TPAT program.
- Negative Vetting: During the vetting negative information regarding the business's import history was found.

Information received from and confirmed to countries with which CBP has a 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; and
- Business identifying numbers, such as:
  - Standard Carrier Alpha Code (SCAC);
  - IOR; and
  - MID.

By Applicant request, information received from, and forwarded to, foreign secure supply chain programs pursuant to a harmonization program may include:

- Legal Name;
- Doing Business As;
- Telephone Number;
- Fax Number;
- Website;
- 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:
  - Type;
  - Name;
  - Country;
  - Street Address;
  - City;
  - State/Province; and
  - Zip/Postal Code.
- Primary Contact:

  - Email Address;
  - Type;
  - Salutation;
  - First Name;
  - Last Name;
  - Title; and
  - 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):
  - Account Number;
  - Risking Status;
  - MSR Status;
  - Validation Type;
  - Validation Closed Date;
  - Validation Status;
  - Validation Type Verification (Government Contact);
  - Verification Type Start Date;
  - Verification Type: (phone, visit, mutual recognition);
  - Verification Visit address;
  - Business Type; and
  - Harmonization Host Program.
- Account Status;
- Vetting Status;
- Minimum Security Requirements/Security Profile Status;
- Validation Status; and
- Harmonization Status.

2.2 What are the sources of the information and how is the information collected for the project?

Information is collected directly from C-TPAT partners or applicants seeking partnership in C-TPAT and indirectly from businesses in the partner's supply chain or through MRAs or memoranda of understanding relating to harmonization efforts. Information may be collected from CBP systems, including TECS, ATS, ACE, and ACS as part of the vetting process undertaken by the SCSS when

verifying the information provided by the applicant/partner. Information may also be collected from publicly available sources using queries of the internet during the vetting and verification process.

Although it is not a requirement of the program that every component of a partner's global supply chain be a C-TPAT partner, the provision of each partner's global supply chain security procedures requires that information about each component/participant in the applicant's SCSP be provided to CBP, even if those supply chain participants are not, or do not desire to become partners of C-TPAT separately. This information is focused on the security procedures of those businesses, rather than the individuals related to those businesses.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Publicly available data queried through the internet is used to verify information provided by the C-TPAT applicant in their SCSP. The SCSS will compare the information provided from the applicant with that available publicly to verify the accuracy of the submitted information and to ensure the applicant can meet basic security criteria. This independent verification is limited to the applicant's supply chain security and does not include non-relevant personal information about individuals related to the business.

2.4 Discuss how accuracy of the data is ensured.

Acceptance into the C-TPAT program requires successful completion of the vetting process, as well as CBP approval of the level of the company's compliance with required Security Criteria. Partners are responsible for filing an accurate SCSP. The system permits partners to alter or file a new SCSP if they find they have submitted inaccurate information. The C-TPAT partner's inputted information is validated by a SCSS. That validation is performed to verify the accuracy of the SCSP information submitted by the applicant/partner. Information from countries with which CBP has an MRA has been validated by that country as part of their secure supply chain program and confirmed by C-TPAT. Information collected through harmonization efforts will be provided by the applicant through the foreign partner and vetted by C-TPAT.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that C-TPAT may collect an unnecessary or excessive amount of PII.

Mitigation: C-TPAT focuses all questions in the application on the business entity, rather than the individual, applying for partnership. When individual information is necessary, such as a point of contact for a business or a sole proprietor, CBP collects and vets only that information necessary to assist in determining the business entity's eligibility. Independent verification using publicly available information is limited to the applicant's supply chain security and does not include non-relevant personal information about individuals related to the business

Privacy Risk: There is a risk that C-TPAT may contain inaccurate information.

Mitigation: C-TPAT mitigates the risk of inaccurate application information by collecting applicant/partner information directly from applicants/partners through the online Security Link Portal wherever possible. Information supplied by countries with which CBP has an MRA is confirmed by CBP. SCSSs are trained to properly evaluate information from other systems during the vetting process to guard against inaccurate information from those systems.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CBP will use the information collected and maintained through the C-TPAT program to administer the C-TPAT program and to carry out its law enforcement and national security missions. Information collected from C-TPAT applicants/partners is used to qualitatively identify those entities whose secure supply chains make them "low risk" of being targets of terrorist or illegal activity within the global supply chain. Information collected from C-TPAT applicants/partners is used 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. Data is also shared pursuant to the routine uses in the C-TPAT SORN.

All companies are vetted by an assigned SCSS prior to being certified or revalidated. Highway Carriers are initially vetted by CBP's Free and Secure Trade (FAST) and then re-vetted and certified by C-TPAT. The SCSS is responsible for vetting the C-TPAT applicant. Vetting is done through queries of various systems, such as ATS, TECS, ACS, ACE and publicly available sources to identify unlawful or suspicious actions involving narcotics, currency, or human smuggling and/or supply chain security-related customs violations, including: hazmat violations, inbond violations, manifesting violations, failing to declare violations, or failure to report violation. A summary of any derogatory information and the resulting analysis of such information by the SCSS will be kept within the internal C-TPAT SharePoint.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. Business-identifying information about partners in C-TPAT, including name and IOR numbers, is provided to ATS in order to reduce the risk score for cargo associated with that business. ATS conducts rule-based targeting to identify high-risk shipments, and C-TPAT lowers the risk scores for participating businesses.[11]

Otherwise, C-TPAT does not conduct electronic search, queries, or analyses to identify a predictive pattern or anomaly. C-TPAT queries internal systems during vetting and to determine the next

[11] See the ATS PIA at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf

supply chain visit. Additionally, C-TPAT is used to query other systems as part of the certification, validation, and evaluation process.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. However, pursuant to the DHS policy for information exchange and sharing, the information collected through the C-TPAT application and verification process may be shared with other component agencies within DHS on a need-to-know basis consistent with the purposes of the original collection. This need-to-know basis must be consistent with the component's legitimate and specific law enforcement or other authorized missions.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse of the information.

Mitigation: To mitigate this risk, internal access to data in C-TPAT is controlled through passwords and restrictive rules. Users are limited to the roles that define their authorized use of the system. CBP uses procedural accountability and physical safeguards, including audit logs and receipt records. Management oversight is in place to ensure appropriate assignment of roles and access to information.

In order to become an authorized user, a CBP employee must have successfully completed privacy training and passed a full field background investigation. In addition, authorized users must have a "need to know" the information for the performance of their official duties. Additionally, all SCSSs receive a two week training session which provides a comprehensive review of the program and identifies SCSS performance expectations. A C-TPAT training manual, which includes instructions for proper information handling procedures, is provided to the SCSSs for use during training and for use as a reference afterward.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

C-TPAT is a voluntary program in which partners must apply. The Security Link Portal and application form (Partner Agreement – See Appendix A) contain a Privacy Act Statement regarding the authority of CBP to collect the requested information and identifying the uses to which the information will be put. Application to the C-TPAT program will constitute consent for use and sharing of the information as outlined in the C-TPAT SORN published in the Federal Register. Additional notice regarding use of C-TPAT information is provided through the publication of this PIA, information on

www.cbp.gov and the notice of proposed rulemaking for the C-TPAT system, published in the Federal Register. A posted privacy policy can be found at the C-TPAT website: https://ctpat.cbp.dhs.gov.

Businesses in an applicant's supply chain may not be provided notice that their information is being provided to CBP by the applicant. However, CBP only asks applicants to provide information about the security procedures they follow with regard to members of their supply chain, not for personal information about those businesses.

Because information collected through MRAs does not come directly from the business, CBP cannot provide notice to companies through MRAs. However, CBP limits the amount of information collected through an MRA to business-identifying information and participation status. CBP is in the process of requiring that countries with which CBP has an MRA ensure foreign manufacturers consent to the sharing of their information with other countries, including the United States.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The C-TPAT program is a voluntary program for enrolled businesses, and the enrollment process involves several steps. Participation in the C-TPAT program requires the applicant to voluntarily provide all requested information to complete enrollment. Prospective applicants may decline to provide information requested by the C-TPAT program application or enrollment process, and thus decline to participate in this voluntary program. A participant may decline to provide required information at any time and elect to cancel the application process or withdraw enrollment. Because of the law enforcement nature of the systems used, some information collected from other sources during the vetting process may be withheld from individuals pursuant to the law enforcement exemptions for C-TPAT and the source systems.

Foreign manufacturers that are not enrolled in C-TPAT, but receive some benefits through participation in a foreign secure supply chain program with which CBP has an MRA, are not able to control their information collected through an MRA. However, CBP limits the amount of information collected through an MRA to business-identifying information and participation status. CBP is in the process of requiring that countries with which CBP has an MRA ensure foreign manufacturers consent to the sharing of their information with other countries, including the United States.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Foreign manufacturers might not know their information has been provided to the United States through a MRA.

Mitigation: CBP limits the amount of information collected through an MRA to business-identifying information and participation status. CBP is in the process of requiring that countries with which CBP has an MRA ensure foreign manufacturers consent to the sharing of their information with other countries, including the United States.

Privacy Risk: Businesses in an applicant's supply chain might not know their information has been provided to CBP via the applicant.

Mitigation: CBP only asks applicants to provide information about the security procedures they follow with regard to members of their supply chain, not for personal information about those businesses.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

CBP is in the process of developing retention requirements for approval by the National Archives and Records Administration (NARA). The information collected through C-TPAT is used for security and risk assessment purposes and data transmitted or copied to the C-TPAT Security Link Portal during the process of vetting a supply chain will be retained in accordance with the record retention period for the C-TPAT SORN. CBP proposes that information stored in C-TPAT be retained for no more than five years beyond the application or partner's enrollment, whichever is longer, and no more than 25 years for any derogatory information.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that PII may be retained in the system for a longer period than is necessary for the purpose for which the information was collected.

Mitigation: Non-derogatory information about a partner is retained in the C-TPAT System to assist with any future related applications for five years after the partner leaves the program. Derogatory information is retained for 25 years to prevent ineligible applicants from later obtaining partnership. Retention of historical information concerning PII and supply chain integrity ensures the ability of the C-TPAT staff to make informed assessments of a C-TPAT Partner's security architecture. Past performance is an important factor in the overall determination of whether an entity may be considered low risk, and thus suitable for inclusion in the C-TPAT program. Retention of this information is consistent with the mission of C-TPAT and necessary for the operation of the validation and subsequent inspection through re-certification process.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, foreign and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. Information may be disclosed from C-TPAT for vetting and supply chain security purposes to federal, state, local, foreign, and private entities in strict compliance with the System of Records Notice, published in the Federal Register. For ad hoc disclosures, requesters outside of DHS must present

a request for a query to the CBP Privacy Office. Upon CBP approval of the specific request, records may be provided either electronically or by hard copy.

Countries that have signed MRAs with CBP may receive confirmation information from C-TPAT. If a foreign manufacturer applies to participate in a foreign secure supply chain program that is the subject of an MRA and is validated, the country with which CBP has a MRA will send the approved company's information with the Manufacturers Identification Number (MID) to C-TPAT. C-TPAT vets the entities using the MID and adjusts the foreign manufacturer's risk assessment. This process saves CBP the time and resources of visiting the foreign company to conduct on-site inspections. C-TPAT does not send any information to countries with which CBP has an MRA, aside from the list of approved foreign manufacturers confirming appropriate adjustments to the completed risk assessment.

CBP plans to pursue harmonization with foreign secured supply chain programs, which would allow C-TPAT partners to share application information and C-TPAT status information located in the C-TPAT Security Link Portal with the foreign secured supply chain program. A harmonization program would similarly allow partners of the foreign supply chain program to share their application and status information with C-TPAT, and this information would be stored in the C-TPAT Security Link Portal. Employees of foreign secure supply chain programs that are part of a harmonization program will be given read-only access to internal and external portions of the C-TPAT Security Link Portal on a need-to-know basis consistent with the routine uses identified in the SORN for C-TPAT. Employees of the foreign supply chain program with such access would be subject to the same requirements as other C-TPAT users.

Release of C-TPAT information by CBP to the public is limited to uses approved by the partner, including the transfer of information by C-TPAT partners within the Status Verification Interface (SVI) and the transfer of other information with C-TPAT partner's consent. Through the internal SVI function, a C-TPAT partner that opts into the SVI function may provide another company its SVI number and retrieve the name of the company and its "certified/non-certified" status. Participation in this function is voluntary, and participants have no obligation to keep confidential the certification status of any participant queried from non-partners. The SCSP of a C-TPAT partner may be released to a third party C-TPAT partner with the authorized consent of the C-TPAT partner about whom the SCSP pertains. This function allows C-TPAT partners to evaluate the security practice of another partner for inclusion in their own supply chain profile.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

As described in Section 6.1, above, PII is shared outside the Department for vetting purposes, in connection with MRAs or harmonization programs with foreign secure supply chain programs, and according to the provisions of the Privacy Act, 5 U.S.C. § 552a, and the routine uses listed in the C-TPAT SORN. Terms and conditions within the C-TPAT partnership agreement outline the scope of information disclosure and are provided upon application to the program (See Appendix A).

6.3 Does the project place limitations on re-dissemination?

Yes. Prior to each sharing of information with a federal, state, or local agency, an MOU or Release Authorization places limitations on the use and re-dissemination of the information. When information is shared with a foreign nation, terms of the sharing provide for limitations on the dissemination of information shared under the MOU.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures outside of the Department require a paper or electronic record to include the date, nature, and purpose of each disclosure as well as the name and address of the individual agency to whom disclosure is made. Paper requests must be approved by the Program Director, and filed. If the request includes PII, the CBP Privacy Officer must approve the release. Requests for information sent via email are processed electronically and stored in a computer database.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is the risk that information shared with external agencies or foreign governments may not be used solely for the purposes for which the information was obtained. Also, there is the risk that the recipient of the information may not maintain adequate safeguarding procedures to protect the information.

Mitigation: Where sensitive C-TPAT information is shared by CBP with a third party (a non-DHS party), it is only done in a manner consistent with the SORN. When sharing within the United States, the recipient must maintain adequate safeguarding procedures for the information and agree that any information obtained would not be shared with any entity without prior notice and the expressed written consent of CBP. Failure to maintain adequate safeguarding procedures may result in termination of future information sharing and/or the administration of civil and/or criminal penalties against involved parties. When sharing with foreign nations, the foreign nation must acknowledge that it will safeguard the information consistent with the laws and policies of its nation.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The C-TPAT Security Link Portal provides access to the information an applicant or partner submitted using their logon user ID and their own unique password. Users create and maintain their own password, which is not disclosed or accessible to the CBP C-TPAT staff. The C-TPAT partner interface allows participants to access and change the information they have provided at any time by accessing

their business identifying information and C-TPAT profile through secure login procedures. C-TPAT Partners access the C-TPAT Security Link Portal via https://ctpat.cbp.dhs.gov.

No exemption shall be asserted 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 applicant's application data and final membership determination in response to a request from that applicant. However, the Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routine uses. Disclosing the fact that a law enforcement agency has sought particular records, including records accessible under the Privacy Act, may affect ongoing law enforcement activity. As such, pursuant to 5 U.S.C. § 552a(j)(2), DHS will claim exemption 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). In addition, to the extent a record contains information from other exempt systems of records, CBP will rely on the exemptions claimed for those systems.

Generally, to gain access to government-held information, individuals may request information about their records contained in C-TPAT through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)). Individuals may seek access to their specific information by filing a FOIA or Privacy Act request in writing, including a daytime phone number and email address. Individuals should provide as much information as possible on the subject matter to expedite the search process. Requests should be sent to:

U.S. Customs and Border Protection
FOIA Division
799 9th Street NW, Mint Annex
Washington, DC 20229-1181

The phone number for the FOIA office is (202) 325-0150. More information is available at http://www.cbp.gov/xp/cgov/admin/fl/foia/reference_guide.xml.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The C-TPAT partner is solely responsible for correcting any erroneous information within their accessible C-TPAT profile. Through the Security Link Portal, C-TPAT partners have a direct messaging option where they may communicate with their assigned SCSS if they believe CBP has acted upon inaccurate or erroneously provided information. If this method is unsuccessful and C-TPAT-facilitated

processing is denied or removed, within 30 days of notification the entity may make written inquiry regarding such denial or removal. The applicant should provide as much identifying information as possible regarding the business, in order to identify the record at issue. C-TPAT participants may provide CBP with additional information to ensure that the information maintained by CBP is accurate and complete. The submitter will receive a written response to each inquiry. If C-TPAT partnership is suspended or removed, the business may appeal this decision to CBP Headquarters, to the attention of the Executive Director, C-TPAT Program Division:

Mr. Daniel Baldwin
Executive Director
Cargo and Conveyance Security
U.S. Customs and Border Protection
1300 Pennsylvania Avenue N.W., Room 2.2A
Washington, D.C. 20229

Individuals may also seek access to their specific information by filing a Freedom of Information Act or Privacy Act request. Businesses may also seek access to records by writing or faxing an inquiry to the U.S. Customs and Border Protection FOIA Division (see 7.1, above).

7.3 How does the project notify individuals about the procedures for correcting their information?

Applicants are provided notice through the Security Link Portal, partnership agreement, and on the C-TPAT website that the C-TPAT partner is solely responsible for correcting any erroneous information within their accessible C-TPAT profile. If an entity believes incorrect or inaccurate information exist, inquiries should be directed to the assigned SCSS or to the Director of the C-TPAT program (See sections 7.1 and 7.2 above). Businesses may also provide additional information if they believe CBP is in possession of inaccurate or erroneous information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is the risk of inaccurate or erroneous information being collected and maintained on individuals.

Mitigation: Any risks associated with redress are mitigated by the applicant's ability to update or delete their information either directly by accessing the C-TPAT web portal or by contacting their assigned SCSS. Any risk that the individual may not be able to correct his information is mitigated by allowing individuals to request access or amendment of their profiles at any time either by contacting an assigned SCSS, or submitting a FOIA/Privacy Act request as outlined on the CBP website. A FOIA reference guide and instructions for filing a FOIA request with CBP can be found at the following link on the CBP.gov website: http://www.cbp.gov/xp/cgov/admin/fl/foia/reference_guide.xml.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Annual security testing is conducted to ensure that applicable security controls are implemented and operating as intended. This includes reviewing user role assignments and associated rules, and ensuring that the C-TPAT system complies with current DHS and CBP policies and procedures.

C-TPAT will assign roles based on the individual's need to know, official duties, agency of employment, and appropriate background investigation and training. C-TPAT user roles are maintained within the application database.

C-TPAT maintains audit trails or logs for the purpose of reviewing user activity. C-TPAT actively prevents access to information for which a user lacks authorization, as defined by the user's role in the system and/or job position. Multiple attempts to access information without proper authorization will cause C-TPAT to suspend access automatically. Security controls generated from DHS, CBP, and NIST 800-53 standards were applied to C-TPAT and thoroughly tested to ensure compliance. The Targeting and Screening Program Office Information Systems Security Officer (ISSO) and ISSO staff review audit logs weekly.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All C-TPAT users undergo initial security awareness training, and thereafter complete the DHS online security awareness-training course annually. Internal CBP C-TPAT users are required to undergo annual privacy training. C-TPAT Partners do not receive security awareness or privacy training. C-TPAT Partners are provided a Notice of Consent on the Applicant Role web page.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to the system is granted and limited to a need-to-know basis. All users with access to data are required to have a positively adjudicated CBP full-field background check, or equivalent. Persons who may have access to the system include C-TPAT partners, CBP Officers, DHS employees, IT specialists, program managers, analysts, and authorized employees of foreign supply chain programs that are part of a harmonization program. Public users fall into three general classes:

Trade Partners - These users consist of three sub-groups that represent users in various stages of the C-TPAT Account lifecycle: Applicants, Certified Partners, and Validated Partners.

- **Applicants** - These users have completed the initial application process and are interacting

with the portal to determine application status and/or provide supplementary information for the application process.

- **Certified Partners** - These users have successfully completed the application process and will be granted access to specified content and tools while they undergo the validation process.
- **Validated Partners** - These users have successfully completed the validation process and will be granted access to specified content and tools requiring the highest security.

C-TPAT Supply Chain Security Specialist Staff (SCSS), Supervisory SCSS - These users will have tools to manage applicant and partner profiles and accounts.

CBP Staff/DHS Headquarters Users - These users will view and utilize data created by C-TPAT supply chain security specialist staff as the specialists assess and administer information received from applicants and partners.

Harmonization Users - Employees of the foreign secure supply chain program will have read-only access to internal and external portions of the C-TPAT Security Link Portal. These users with such access will be subject to the same or equivalent requirements as other internal C-TPAT users.

Access to the system for internal users is limited to a need-to-know basis. All internal users with access to the system are required to have completed full field background investigations and must receive authorization by the C-TPAT Security Administrator in order to have general access to the system. All CBP user roles and access requests are vetted through the Program Manager. If approval is granted by the program manager, information is forwarded to the system administrator, who will create the user account only after background information has been verified.

8.4 How does the project review and approve information sharing arrangements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All C-TPAT memoranda of understanding (MOU) are created by the C-TPAT administrators and approved by the Office of Chief Counsel and the Office of International Affairs. MOUs related to C-TPAT do not include the transmission of PII. However, if a C-TPAT MOU is developed in the future and does contain provisions for the transmission of PII, it will be sent to the CBP Privacy Officer for review and to DHS for final approval.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
U.S. Customs and Border Protection
(202) 325-0280

Shawn Beddows
Acting C-TPAT Director
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-2619

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

APPENDIX A

CTPAT-Partner Agreement to Voluntarily Participate

This Agreement is made between **CTPAT Partner Company** (hereafter referred to as "the Partner") and U.S. Customs and Border Protection (hereafter referred to as "CBP").

This Agreement between the Partner and CBP will enhance the joint efforts of both entities to better secure the international supply chain to the United States. CBP and the Partner recognize the need to improve and expand existing security practices in order to achieve a more efficient and compliant import process.

The Partner agrees to develop and implement, within a framework consistent with the listed CTPAT criteria, a verifiable and documented program to enhance security procedures throughout its supply chain. Where the Partner does not exercise control of a production facility, distribution entity, or process in the supply chain, the Partner agrees to communicate the CTPAT criteria to those entities.

Specifically, the Partner agrees to:

1. Commit to working with business partners and CBP to meet CTPAT minimum security criteria.
2. Using the online application process (the CTPAT Portal), complete a supply chain security profile and update information regarding the company on an annual basis.
3. Provide complete and accurate company information in response to CTPAT inquiries.
4. Comply with CTPAT program requirements to ensure integrity at each stage of the Partner's supply chain.
5. Cooperate with the CTPAT validation process including assisting the CBP Supply Chain Security Specialists (SCSS) in planning for and conducting site visits.
6. Acknowledge and cooperate with re-validation procedure as deemed necessary by CBP.
7. Maintain security integrity throughout the partnership, conducting periodic self-assessments in line with the changing risks and complexity of international business and trade.
8. Cooperate with CBP, domestic and foreign port authorities, foreign customs administrations and others in the trade community, in advancing the goals of CTPAT and the Container Security Initiative (CSI).
9. Acknowledge and accept this Agreement to Voluntarily Participate by marking the "I agree" box below.

Upon acceptance, review, and/or certification in the CTPAT program, CBP will:

1. Assign a Supply Chain Security Specialist (SCSS) to work individually with the Partner in CTPAT procedures.
2. Review the Partner's CTPAT application within 90 days of receipt.
3. Conduct a CTPAT validation within one year of the Partner's CTPAT certification in accordance with section 215 (a) of the "Security and Accountability for Every Port Act of 2006" (SAFE Port

Act), Pub. L. 109-347, 120 Stat. 1917. CBP will, to the extent possible, be flexible to the Partner's scheduling availability.

4. Provide the Partner with feedback regarding the validation including any security enhancement recommendations, actions required, and recognition of CBP identified best practices.
5. Endeavor to assist the Partner with security threat awareness training and in identifying high risk factors specific to the Partner's operating environment(s).
6. Not request that the Partner take any action which would conflict with any U.S. laws or regulations relevant to the Partner's operations.
7. Provide CTPAT participant verification capability via the Status Verification Interface (SVI).
8. Conduct re-validations in accordance with time frames set forth in section 219 of the SAFE Port Act.
9. Allow the Partner a reasonable timeframe within which to comply with and/or implement security practices or measures that represent an amendment or change to current CTPAT imposed requirements.
10. Where feasible and to the extent practical, extend specific CTPAT benefits to Partners at U.S. ports of entry.
11. Provide the opportunity for CTPAT Partners to be eligible to participate in the developing Mutual Recognition Program by exchanging information with foreign administrations, which may enable CTPAT partners to receive more benefits, but only through prior consent of the CTPAT member.

CBP acknowledges that during the course of the CTPAT membership relationship between CBP and the Partner, CBP may become privy to proprietary business information. CBP recognizes the confidential nature of such information, and agrees to take the appropriate measures to maintain the confidentiality of this information in accordance with U.S. law.

This Agreement is subject to review by the Partner or CBP and may be terminated with written notice by either party.

This Agreement cannot, by law, exempt the Partner from any statutory or regulatory sanctions in the event that discrepancies are discovered during a physical examination of cargo or the review of documents associated with the Partner's CBP transactions.

Nothing in this Agreement relieves the Partner of any statutory or regulatory responsibilities under United States law, including any requirements imposed under DHS and CBP statutes and regulations.

Agree □

_____
Company Name

_____ _____

Company Principle or Representative Date

_____ _____
On behalf of CBP Date

Position and contact information:

APPENDIX B

Foreign secure supply chain programs with which CBP has signed Mutual Recognition Arrangements

As of April 12, 2020, CBP has signed 12 MRA's:

- New Zealand - June 2007 – New Zealand Customs Service's Secure Export Scheme Program
- Canada - June 2008 – Canada Border Services Agency's Partners in Protection Program (PIP)
- Jordan - June 2008 – Jordan Customs Department's Golden List Program
- Japan - June 2009 – Japan Customs and Tariff Bureau's Authorized Economic Operator Program
- Korea - June 2010 – Korean Customs Service's Authorized Economic Operator Program
- European Union - May 2012 – European Union's Authorized Economic Operator Program
- Taiwan - November 2012– Directorate General of Customs, Taiwan Ministry of Finance's – Authorized Economic Operator Program*
- Israel – June 2014 - Israel Tax Authority's Authorized Economic Operator Program.
- Mexico - October 2014 - Mexico Tax Administration Service Mexico AEO
- Singapore – December 2014 – Singapore Customs' Secure Trade Partnership (STP) Program
- Dominican Republic - December 2015 – Authorized Economic Operator Program – AEO
- Peru - September 2018 - Authorized Economic Operator Program

Foreign secure supply chain programs with which CBP has harmonized CTPAT:

- Canada – Canada Border Services Agency's Partners in Protection Program (PIP)

APPENDIX C

General Application Instructions

http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_application_material/applying_for_ctpat/applying_for_ctpat_online/general_application_instructions.ctt/general_application_instructions.pdf

Highway Carrier

http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_application_material/applying_for_ctpat/applying_for_ctpat_online/hwy_carrier_app_instructions.ctt/hwy_carrier_app_instructions.pdf

Third Party Logistics Providers and Consolidators

http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_application_material/applying_for_ctpat/applying_for_ctpat_online/3plp_app_instructions.ctt/3plp_app_instructions.pdf