THOMSON REUTERS PRACTICAL LAW

Customs Trade Partnership Against Terrorism: A Guide for US Importers

by Practical Law Commercial Transactions

Maintained • USA (National/Federal)

Related Content

A Practice Note describing the Customs Trade Partnership Against Terrorism (CTPAT) as it relates to US importers. This Note discusses the eligibility requirements and minimum security criteria that importers must meet to be certified as a member of CTPAT by US Customs and Border Protection (CBP) and the benefits that importers may receive from CBP in return for their implementation of measures to maintain the security of the international supply chain.

This resource is being updated to reflect CBP's updates to its CTPAT minimum security crtiteria for importers (see Legal Update, US Customs and Border Protection Issues Updated CTPAT Minimum Security Criteria).

The Customs Trade Partnership Against Terrorism (CTPAT) was established by the US Customs Service, the predecessor of **US Customs and Border Protection** (CBP), in response to the terrorist attacks of September 11, 2001.

First announced in November 2001, formally implemented in April 2002, and eventually codified into law by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (6 U.S.C. §§ 961 to 973), CTPAT is a voluntary incentives-based program in which CBP works with members of the international trade community to strengthen international supply chain security and prevent the supply chain from being compromised by terrorist organizations.

In return for ensuring that their supply chain security practices meet certain minimum security criteria established by CBP, importers that are accepted into the program are eligible to receive various benefits from CBP, including:

- Reduced examination rates.
- Expedited processing of shipments.

CBP reduces screening of imports by companies that are CTPAT certified because it considers these importers to be low risk.

CTPAT membership is also available to other stakeholders in the international supply chain, such as:

- US exporters.
- Licensed US customs brokers.
- Mexican and Canadian manufacturers.
- Sea carriers transporting cargo to the US.
- Air carriers transporting cargo to the US.
- Rail carriers transporting cargo to or from Canada or Mexico.
- Highway carriers transporting cargo to or from Canada or Mexico.
- Long-haul carriers in Mexico.

- Consolidators, including:
  - air freight consolidators;
  - ocean transportation intermediaries; and
  - non-vessel operating common carriers (NVOCCs).
- US marine or port terminal operators (MPTO) and certain foreign-based MPTOs.
- Federally licensed or bonded third-party logistics providers (3PL).

This Practice Note discusses the CTPAT program as it relates to US importers. The eligibility requirements and minimum security criteria for other stakeholders in the international supply chain are not discussed in this Note. For more information on those requirements and criteria, see CBP: CTPAT Minimum Security Criteria and Guidelines.

As of the end of Fiscal Year 2016, CBP has certified more than 11,500 companies for CTPAT membership, almost 40 percent of which are importers. CBP encourages all companies that regularly import goods into the US to apply for CTPAT membership.

Importer Eligibility Requirements

To be eligible to participate in CTPAT, an importer must:

- Be an active US importer or non-resident Canadian importer. Companies must have imported goods into the US within the past year.
- Have a business office staffed in the US or Canada.
- Have an active US importer of record identification number.
- Have a valid continuous customs bond registered with CBP.
- Designate a company officer to be the primary cargo security officer responsible for C- TPAT.
- Sign an agreement to voluntarily participate in the program.
- Create and provide CBP with a CTPAT supply chain security profile that identifies how the importer will meet, maintain, and enhance the CTPAT importer security criteria.
- Pass a validation of its security procedures that CBP will conduct at selected domestic and foreign facilities.

If CBP accepts an importer into CTPAT, CBP will assess the importer's program eligibility and security profile annually and generally will revalidate the importer's security procedures every three years. For more information on the annual eligibility review, the annual security profile review, and revalidations, see Practice Note, Customs Trade Partnership Against Terrorism: Post-Validation Proceedings: Annual Reviews by CBP and Revalidations.

Benefits from Participation

As an incentive for importers to implement the supply chain security measures desired by CBP, CBP offers several benefits to importers that are accepted into the program, including:

- A reduced number of CBP examinations. However, importers should note that if a CTPAT member's cargo is imported in a consolidated load, that is, in the same container with cargo imported by another party, and CBP believes the other party's cargo is higher risk warranting an examination, CBP will examine the entire shipment.
- Shorter wait times at the border and front of the line inspections. To the extent practicable, CTPAT importers' shipments are moved ahead of non-CTPAT importers' shipments.
- Access to Free and Secure Trade (FAST) lanes. FAST lanes are dedicated highway lanes available to CTPAT members at many land border ports of entry that allow expedited border crossing privileges.
- Assignment of a CBP Supply Chain Security Specialist. The Supply Chain Security Specialist assists the CTPAT member with supply-chain-security-related issues and helps the importer maintain compliance with CTPAT requirements and continued membership in the program.

- Access to the online CTPAT Portal and library of training materials.
- Eligibility to attend CTPAT conferences and other training seminars.
- Possible additional benefits by being recognized as a trusted trader by foreign customs administrations that have signed Mutual Recognition Arrangements (MRA) with CBP (see Mutual Recognition Arrangements (MRA)).
- Eligibility for other US government pilot programs, such as the Food and Drug Administration's Secure Supply Chain program.
- Business resumption priority if there is a significant disruption or delay in CBP cargo processing operations following a natural disaster or terrorist attack.
- A stratified exam benefit. If only one container of a multi-container shipment is to be examined, the importer may move the other containers to its premises provided they remain sealed and available for inspection if CBP determines further inspection to be necessary after its examination of the targeted container.
- Eligibility to participate in CBP's Importer Self-Assessment program (see Importer Self-Assessment Program).
- Priority consideration by CBP's Centers of Excellence and Expertise in the resolution of trade compliance and admissibility issues at ports of entry (see Centers of Excellence and Expertise).

Importer Self-Assessment Program

CTPAT members are eligible to participate in CBP's Importer Self-Assessment (ISA) program. The ISA is a voluntary program open only to CTPAT members with at least two years of importing history. To participate, importers must complete an ISA application and be approved by CBP. The ISA program allows importers to assess and monitor their own compliance with CBP laws and regulations in return for various benefits, including:

- Exemption from certain compliance audits (Focused Assessments).
- Expedited treatment of requests for CBP ruling letters (see Practice Note, US Customs Advance Ruling Letters).
- Enhanced ability to receive prior disclosure treatment under 19 C.F.R. Section 162.74 (see 67 Fed. Reg. 41298 at 41299).
- Assignment of a National Account Manager to assist in resolving CBP-related issues.
- Consideration of the importer's ISA participation as a mitigating factor if penalties or liquidated damages are assessed against the importer.

Centers of Excellence and Expertise

CTPAT members are also entitled to priority consideration by CBP's Centers of Excellence and Expertise (CEEs) in the resolution of trade compliance and admissibility issues at ports of entry. CBP has established ten CEEs to provide centralized trade processing functions on an industry-wide basis to increase uniformity of practice at the port level and facilitate the resolution of compliance issues nationwide. The CEEs, which are staffed by CBP personnel nationwide who operate in a virtual environment, are coordinated from various locations around the country as follows:

- Apparel, footwear, and textiles (San Francisco).
- Electronics (Los Angeles).
- Machinery (Laredo).
- Petroleum, natural gas, and minerals (Houston).
- Base metals (Chicago).
- Consumer products and mass merchandising (Atlanta).
- Industrial and manufacturing materials (Buffalo).
- Automotive and aerospace (Detroit).
- Agriculture and prepared products (Miami).
- Pharmaceuticals, health, and chemicals (New York).

Tiered Benefits Structure

CBP employs a tiered benefits structure that assigns CTPAT members Tier I, Tier II, or Tier III status, with Tier III members entitled to the most benefits (see Tier I Status, Tier II Status, and Tier III Status). The stratified exam benefit and eligibility for the FDA's Secure Supply Chain program are limited to Tier II and Tier III importers. The stratified exam benefit also requires that importers participate in the ISA program.

Government Accountability Office Study

In February 2017, the US Government Accountability Office (GAO) issued the results of an audit of the CTPAT program to determine the extent to which CTPAT members receive benefits, such as:

- Reduced likelihood of CBP examinations.
- Expedited shipment processing, compared to non-CTPAT members (see GAO: Supply Chain Security: Providing Guidance and Resolving Data Problems Could Improve Management of the Customs Trade Partnership Against Terrorism Program).

The GAO reported CBP data showing that:

- CTPAT certified importers are four to six times less likely to undergo a CBP security or trade compliance examination than are non-CTPAT members.
- Tier III importers are nine times less likely to undergo a CBP security-based examination.

However, the GAO found that due to problems with CTPAT's data management system, CBP cannot:

- Determine the extent to which CTPAT members are receiving benefits, such as reduced likelihood of cargo examinations and expedited shipment processing, compared to nonmembers.
- Be assured that CTPAT members have consistently received the benefits that CBP has publicized.

The GAO further noted that when it compared the examination rates of CTPAT members' shipments with those of nonmembers, CTPAT program data showed that CTPAT members did not consistently experience lower examination rates, hold rates, and processing times compared to nonmembers' shipments across the various modes of transportation (air, truck, vessel, and rail). However, the GAO reported that industry officials it met with generally spoke positively of the program.

CTPAT officials are finalizing an action plan to correct the data concerns and are reported to be exploring new benefits for CTPAT members.

Supply Chain Risk Assessment

Before applying for CTPAT membership, an importer must:

- Review the CTPAT minimum security criteria (see CTPAT Importer Minimum Security Criteria).
- Conduct a comprehensive self-assessment of the risks in its supply chain, including an evaluation of its business partners' security procedures (see Business Partner Requirements).

In conducting the risk assessment, importers must determine:

- The security risks that exist in their international supply chain, including foreign manufacturers, freight forwarders, carriers, and warehouses.
- How they mitigate those risks.

CBP recommends a five-step risk assessment in which importers:

- Map the flow of cargo through their supply chain, identifying all:
  - modes of transportation; and
  - business partners involved in the movement of cargo from the point of manufacture to the point of distribution in the US.
- Conduct a threat assessment by country and region that identifies threats to the supply chain. The threat assessment should assign a risk rating of low, medium, or high in the areas of:
  - terrorism;

    - contraband smuggling;
    - human smuggling;
    - agricultural and public safety threats; and
    - organized crime.
- Conduct a vulnerability assessment of the supply chain based on the CTPAT minimum security criteria. The vulnerability assessment should identify weaknesses in security procedures that can be exploited by terrorists and other criminals identified in the threat assessment. The vulnerability assessment may involve:
    - an internal audit of the importer's security policies and procedures;
    - the issuance of security questionnaires to the importer's supply chain business partners; and
    - security audits and site visits to the importer's supply chain business partners.
- Prepare a written action plan to address the vulnerabilities identified in the vulnerability assessment. The action plan should:
    - identify procedures to reduce the vulnerabilities. For example, the importer may post an employee at a high-risk foreign manufacturer. In some situations, an importer may conclude that the risks are too high to commence or continue a relationship with a particular business partner;
    - identify the personnel that will be responsible for implementing the procedures;
    - set due dates for taking corrective action; and
    - provide for verification that the corrective action has been taken.
- Document, review, and periodically revise the procedure for conducting the risk assessment. The risk assessment should be performed at least annually and more frequently for high-risk supply chains.

(See CBP: CTPAT's Five Step Risk Assessment.)

Application Process

An importer applies for CTPAT membership by submitting an application by a web portal (CTPAT Portal) on CBP's website (see CBP: CTPAT Portal Login and CBP: CTPAT Portal User Manual). The application includes:

- A company profile containing general information about the importer (see Company Profile).
- A security profile of the importer's supply chain (see Security Profile).

As part of the application, an officer of the company must electronically sign the CTPAT partner agreement, acknowledging the importer's voluntary participation in the program and its agreement to meet CTPAT requirements. If an importer is admitted to the CTPAT program and subsequently fails to uphold its commitments, CBP may suspend benefits or cancel the importer's participation in the program. For more information on the CTPAT enforcement process, see Practice Note, Customs Trade Partnership Against Terrorism: Post-Validation Proceedings: Suspension, Removal, Appeals, and Reinstatement.

Before completing the application itself, an importer must create a Trade Account containing an organization profile consisting of:

- Company information, such as the importer's:
    - name;
    - doing business as name;
    - telephone and fax numbers;
    - website;
    - business start date;
    - number of employees; and

    - company history.
- Addresses related to:
    - headquarters offices;
    - trade and security points of contact and office locations;
    - import and export cargo handling facility locations; and
    - policy generation and training locations.
- User information for all persons who will have access to the importer's CTPAT Portal account.

After an importer creates a Trade Account, it proceeds to the CTPAT application consisting of the company profile and the security profile.

Company Profile

The company profile contains information related to the importer's CTPAT account, including:

- Business type. Applicants must confirm that they are the type of entity that is eligible to participate in CTPAT by indicating whether they are applying as an importer, customs broker, highway carrier, consolidator, or other specified eligible entity.
- Business entity information, such as the Importer of Record Number.
- Addresses. These include a primary address, mailing address, and all other addresses previously entered into the organization profile section of the Trade Account that the importer wants associated with its CTPAT application.
- Contacts. These are the appropriate CTPAT contacts previously entered into the organization profile that the importer wants associated with its CTPAT application. The importer must also designate a primary point of contact, which may be either a company officer or an employee.

After the importer submits the company profile, the system creates an account for the importer in the CTPAT Portal. The importer can then proceed to enter information into the security profile.

Security Profile

The importer's security profile requires detailed written information on the security measures and procedures that are used in the importer's supply chain. For CTPAT, the supply chain extends from the point of origin (manufacturer, supplier, or vendor) through each transportation link until the cargo reaches the final distribution point in the US and is unloaded from the conveyance.

To complete the security profile, the importer must submit information regarding its security processes and procedures for eight major categories into which the CTPAT minimum security criteria for importers is divided (see CTPAT Importer Minimum Security Criteria). The categories are:

- Business partner requirements (see Business Partner Requirements).
- Container security (see Container Security).
- Physical access controls (see Physical Access Controls).
- Personnel security (see Personnel Security).
- Procedural security (see Procedural Security).
- Security training and threat awareness (see Security Training and Threat Awareness).
- Physical security (see Physical Security).
- Information technology security (see Information Technology Security).

For each category, the importer must provide its response or upload a document, or both, that demonstrates how it meets the particular CTPAT minimum security criteria. CBP reviews the submitted information and assesses whether the security profile adequately addresses the CTPAT minimum security criteria for importers (see CBP Review of Application).

CTPAT Importer Minimum Security Criteria

The importer must ensure that appropriate security measures are implemented throughout the supply chain for each security category. This may be achieved by doing business, to the greatest extent possible, with companies that are themselves CTPAT certified or whose security practices have been certified by an equivalent security program administered by a foreign customs authority (see Mutual Recognition Arrangements (MRA)).

Importers may use the Status Verification Interface (SVI) tool in the CTPAT Portal to facilitate the screening and monitoring of their business partners for CTPAT compliance (see Business Partner Requirements).

If an importer does business with companies that are not members of CTPAT or an equivalent foreign program recognized by CBP, the importer must be aware of the security measures used by those business partners and have a documented risk assessment process in place to verify that these business partners comply with CTPAT security criteria.

Importers must also perform periodic reviews of these business partners' processes and conduct on-site security assessments of their facilities, based on the level of risk. CBP expects importers to work with their business partners, including those whose facilities or operations may not be under the importer's direct control, to improve any areas where security deficiencies exist (see CBP: Importer Frequently Asked Questions).

Business Partner Requirements

Importers must have written and verifiable processes for:

- Selecting their business partners, including manufacturers, suppliers, logistics providers, and vendors.
- Ensuring their business partners develop security procedures consistent with CTPAT minimum security criteria applicable to the business partner.

Internal selection criteria should include consideration of a business partner's:

- Financial soundness.
- Ability to meet contractual security requirements.
- Ability to identify and correct security deficiencies as necessary.

Importers must also require their business partners to demonstrate that they have security processes and procedures consistent with the CTPAT security criteria by providing certain documentation to the importer. The type of documentation varies depending on whether the business partner is:

- Eligible to participate in CTPAT. If so, the importer must obtain documentation indicating whether the business partner is CTPAT certified, such as:
    - a CTPAT certificate issued by CBP; or
    - an SVI number. The SVI number is an identification number that CBP assigns to CTPAT participants that consent to the release of their company's name and CTPAT status to other consenting CTPAT participants (see CBP: CTPAT Status Verification Interface).
- Not eligible to participate in CTPAT. If so (or if the business partner is eligible to participate but is not a CTPAT member), the importer must require the business partner to provide written or electronic confirmation that they meet CTPAT security criteria, for example:
    - contractual obligations;
    - a letter from a senior officer of the business partner attesting to CTPAT compliance;
    - a written statement from the business partner demonstrating compliance with CTPAT security criteria or an equivalent World Customs Organization (WCO)-accredited security program administered by a foreign customs authority; or
    - a completed security questionnaire issued by the importer.

Container Security

CBP requires that shipping container security be maintained at the point of stuffing to protect against the introduction of unauthorized material or access by unauthorized persons. The elements of container security include container:

- Inspection. Procedures must be in place to verify the physical integrity of the container structure before stuffing, including the reliability of the locking mechanisms for the doors. CBP recommends a seven-point inspection of the container's:
    - front wall;
    - left side;

- right side;
- floor (inside);
- undercarriage;
- ceiling and roof; and
- inside and outside doors.

- Seals. Procedures must be in place to properly maintain the integrity of shipping containers, including:
  - affixing a high-security seal to all loaded containers bound for the US. The seal must meet or exceed the current Publicly Available Specifications (PAS) of the International Organization for Standardization (ISO) for mechanical seals that are acceptable for securing freight containers in international commerce, specifically, the current PAS ISO 17712 standards for high-security seals; and
  - adopting written procedures that specify how seals are to be controlled and affixed to loaded containers (for example, only designated employees should be permitted to distribute container seals) and how compromised seals or containers are to be reported to CBP or the appropriate foreign authority.
- Storage. Containers must be stored in a secure area to prevent unauthorized access or manipulation, and procedures must be in place to report and neutralize unauthorized entry into either the containers or the storage area.

Physical Access Controls

Importers must ensure that procedures are in place to control access and prevent unauthorized entry into company facilities. Access controls must include a system for the positive identification of:

- Employees. Companies should give their employees access only to those areas needed for the performance of their duties.
- Visitors. Companies must:
  - require visitors to present photo identification on their arrival;
  - issue temporary identification to visitors;
  - require visitors to display the temporary identification issued to them; and
  - ensure that company personnel escort visitors while they are on company grounds.
- Vendors. Companies should:
  - require delivery personnel (including mail carriers) and other vendors to present vendor or photo identification on their arrival; and
  - implement procedures to periodically screen arriving packages and items received by mail before they are distributed.

Company management or security personnel must adequately control and document the procedures for issuing, changing, and removing employee, visitor, and vendor identification badges and access devices, such as keys or key cards.

Importers must also ensure that procedures are implemented to identify, challenge, and address all unauthorized or unidentified persons.

Personnel Security

Processes must be established for:

- Pre-employment screening and verification. These include procedures for:
  - reviewing the information provided in the job application, such as employment history;
  - verifying references; and
  - conducting background checks, consistent with foreign, federal, state, and local regulations. Importers should document any limitations imposed by law.
- Periodic checks and reinvestigations of current employees based on cause or the sensitivity of the employee's position.

- The termination of employees. Companies must have procedures for removing employee identification and canceling facility and systems access when an employee resigns or is terminated.

Procedural Security

Importers must ensure that measures are in place to safeguard the secure transportation, handling, and storage of cargo in the supply chain. These procedures should cover:

- Document processing and control. Procedures must be in place to ensure that all information used in clearing cargo through CBP is:
  - legible, complete, and accurate; and
  - protected against the exchange, loss, or introduction of erroneous information. This includes safeguarding computer access and electronically stored information.
- Manifesting procedures. Procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.
- Shipping and receiving. Procedures should be implemented to ensure that:
  - arriving cargo is described accurately and reconciled against information on the cargo manifest, and its weights, labels, marks, and piece count are properly indicated and verified;
  - departing cargo is verified against purchase or delivery orders; and
  - drivers delivering or receiving cargo are positively identified before cargo is received or released.
- Cargo discrepancies. Procedures must be implemented to ensure that:
  - shortages, overages, and other significant discrepancies are investigated and resolved appropriately; and
  - CBP or other law enforcement agencies, or both, are notified if illegal or suspicious activities are detected, as appropriate.

Security Training and Threat Awareness

Security personnel should establish and maintain a program to:

- Foster awareness of the threat posed by terrorists at each point in the supply chain.
- Make employees aware of the company's procedures for reporting and addressing security threats. Shipping and receiving personnel and mailroom employees should receive additional training in this area.
- Offer specialized training, tailored to the security-related tasks performed by the various types of employees of the company, to help employees maintain cargo integrity, recognize internal conspiracies, and protect access controls. Companies should offer incentives to encourage employee participation.

Physical Security

Cargo handling and storage facilities in the US and foreign countries must have physical barriers and deterrents to guard against unauthorized access. Importers should ensure that measures are implemented throughout their supply chains to safeguard the security of buildings and surrounding property. These include adequate and secure:

- Fencing. Importers should ensure that:
  - perimeter fencing encloses the areas around cargo handling and storage facilities;
  - interior fencing is used in cargo handling buildings to segregate domestic, international, high value, and hazardous cargo; and
  - fencing is inspected regularly for structural integrity and damage.
- Access gates and gate houses. Gates through which vehicles or personnel enter and exit must be manned or monitored, or both. The number of gates should be kept to the minimum necessary for proper access and safety.

- Parking facilities. Private passenger vehicles should be prohibited from parking in or next to cargo handling and storage areas.
- Building structure. Importers must ensure that buildings are:
  - constructed of materials that resist unlawful entry; and
  - periodically inspected and repaired as necessary to maintain structural integrity.
- Locking devices and key controls. All external and internal windows, gates, and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.
- Lighting. Adequate interior and exterior lighting must be provided, including lighting for:
  - entrances;
  - exits;
  - cargo handling and storage areas;
  - fence lines; and
  - parking areas.
- Alarm systems and video surveillance cameras. Alarms and video cameras should be used to:
  - monitor the premises; and
  - prevent unauthorized access to cargo handling and storage areas.

Information Technology Security

Importers must ensure that information technology (IT) policies and procedures are in place for:

- Password protection and monitoring the integrity of business data. Companies should have:
  - automated systems that use individually assigned accounts that require a periodic change of password; and
  - written IT policies, procedures, and standards that are provided to employees as part of training.
- Ensuring accountability. Companies must implement a system to identify IT abuses, including:
  - improper access; and
  - tampering or altering business data.

Employees that violate IT procedures must be subject to appropriate disciplinary action.

CBP Review of Application

After the importer populates the security profile with information regarding the security measures for each security category and submits the application, CBP assigns the importer a Supply Chain Security Specialist (SCS Specialist). The SCS Specialist reviews the submitted information (along with the importer's customs compliance history) and assesses whether the security profile adequately addresses the CTPAT minimum security criteria for importers.

If the SCS Specialist approves the application, including the security profile, the importer is accepted into the CTPAT program (that is, certified as a CTPAT member) and is eligible to receive certain benefits (see Acceptance into CTPAT and Tier I Status).

Thereafter, CBP will conduct on-site visits, known as validations, to verify that the security measures described in the security profile have been implemented (see CTPAT Validation). A successful validation will result in an importer being eligible for increased benefits, either Tier II benefits or, in rare cases, Tier III benefits (see Tier II Status and Tier III Status). If the validation reveals significant weaknesses, the importer's benefits (which were at the Tier I level going into the validation) may be suspended pending corrective action.

Acceptance into CTPAT

Under the SAFE Port Act, to the extent practicable, CBP has 90 days to certify a company as a CTPAT member or reject its application. If an importer's application, including its security profile, is approved, the importer is accepted into the CTPAT program, is assigned Tier I status, and begins receiving benefits as a Tier I importer.

Tier I Status

Tier I importers receive reduced risk scores under CBP's Automated Targeting System (ATS), which uses a mathematical model to help prevent terrorists and terrorist weapons from entering the US. The ATS analyzes shipping information, such as cargo manifests submitted by ocean carriers, and entry data submitted by importers to assign a risk score to arriving shipments that helps CBP identify containers for examination.

Lower risk scores assigned to Tier I importers result in:

- Fewer cargo examinations by CBP for security concerns.
- A lower level of random CBP compliance measurement examinations than are conducted for non-CTPAT members.

Tier I importers are also eligible for:

- Expedited cargo processing at FAST lanes at US land borders.
- Front of the line inspection privileges at ports of entry if an examination is required.
- Participation in the ISA program.
- CTPAT training seminars.

CTPAT Validation

Under the SAFE Port Act, to the extent practicable, CBP must verify the importer's security profile within one year after certifying the importer as a CTPAT member.

After an importer is accepted into the CTPAT program, the SCS Specialist will contact the importer to arrange visits to selected domestic and foreign facilities in the importer's supply chain to observe security practices. These are known as validation visits. CBP provides companies approximately 30 days advance written notice.

If CBP confirms through its validation visits that the supply chain security measures meet the CTPAT minimum security criteria, the importer will be assigned Tier II Status and begin receiving commensurate benefits (see Tier II Status).

If CBP determines in the validation visits that the importer's supply chain security measures exceed the CTPAT minimum security criteria and rise to the level of best practices, CBP will assign the importer Tier III status and provide commensurate benefits (see Tier III Status).

Under the SAFE Port Act, CBP must revalidate all CTPAT participants at least once every four years. CBP generally revalidates companies every three years.

On-Site Visits

In a validation, a CBP team (usually led by the SCS Specialist assigned to the importer) meets with the importer's representatives and visits domestic and foreign sites that are selected based on the SCS Specialist's risk analysis to verify that the supply chain security measures described in the security profile:

- Are accurate.
- Meet the CTPAT minimum security criteria.
- Are being followed.

Domestic site validations may include the importer's:

- Corporate headquarters.
- Warehouses and distribution centers.

Foreign site validations may include:

- Manufacturers or suppliers.
- Freight forwarders.
- Consolidation facilities.

Mutual Recognition Arrangements (MRA)
If a foreign business partner, such as a manufacturer, is an Authorized Economic Operator (AEO), that is, a foreign customs administration has approved the company as complying with WCO or equivalent supply chain security standards as well the foreign country's customs laws and regulations, CBP may recognize the foreign customs administration's security validation findings instead of conducting its own visit if both:

- The AEO program has security requirements and validation standards that are the same as or similar to CTPAT requirements.
- CBP has signed an MRA with the other country's customs administration.

However, CBP still reserves the right to conduct a validation visit to these facilities.

As of the end of Fiscal Year 2016 (stated in chronological order), CBP has signed MRAs with:

- New Zealand.
- Canada.
- Jordan.
- Japan.
- South Korea.
- The European Union.
- Taiwan.
- Israel.
- Mexico.
- Singapore.
- The Dominican Republic.

Validation Report

After the validation visits, CBP briefs the importer's management on the validation's findings and shortly thereafter provides the company with a written report containing CBP's findings. Depending on the results of the validation, the report may:

- Include recommendations for improving security practices.
- Identify actions that the importer must take to meet the CTPAT minimum security criteria.
- Conclude that the importer is entitled to receive Tier II benefits (see Tier II Status).
- If appropriate, identify security procedures that qualify as best practices and assign Tier III status (see Tier III Status).

If the validation reveals significant weaknesses in security practices, CBP may suspend the importer's benefits. If CBP suspends an importer's benefits, CBP will recommend a corrective action plan to address the weaknesses that were identified. Benefits may be reinstated when corrective action is implemented and verified.

Tier II Status

If the validation findings confirm that an importer meets the minimum CTPAT security criteria, the importer is assigned Tier II status and begins receiving increased benefits. Tier II benefits include:

- All Tier I benefits.

- Twice the level of risk score reductions received by Tier I importers, resulting in even fewer CBP exams for security reasons.

Tier III Status

Importers are granted Tier III status if their security practices are both:

- Validated as exceeding the CTPAT minimum security criteria (see CTPAT Importer Minimum Security Criteria).
- Considered by CBP to be best practices.

Tier III benefits include:

- All Tier I and Tier II benefits.
- The most significant risk score reductions available, resulting in very infrequent CBP examinations for security reasons.

To qualify as a CTPAT best practice, a supply chain security measure must:

- Be innovative and exceed the CTPAT minimum security criteria.
- Incorporate senior management support.
- Have written and verifiable processes that govern its use.
- Employ a system of checks and balances.
- Have measures in place to ensure continuity.

For examples of best practices in each of the eight major security criteria categories, as identified by CBP while conducting validations, see CBP: CTPAT Best Practices.

To date, several hundred importers have attained Tier III status.

PRODUCTS

PLC US Commercial Transactions, PLC US Law Department