Office of Field Operations

Customs Trade Partnership Against Terrorism (CTPAT)

CTPAT Program Overview

CTPAT Program Overview

CTPAT is a voluntary public-private sector partnership program to strengthen the security of international supply chains and the U.S. Border, and increase trade compliance.

Trade Security

Trade Security refers to the security of supply chains relative to current and emergent threats.
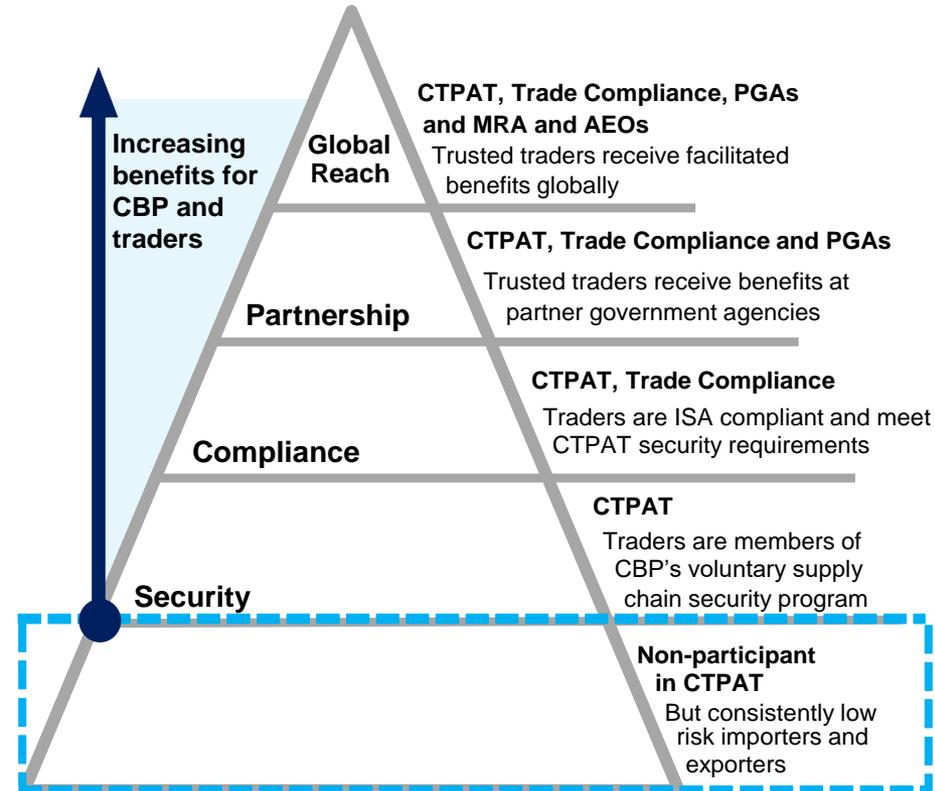
- CBP partners with industry and foreign governments, and uses a risk-based approach to identify threats at the earliest point possible and before they reach U.S. Ports of Entry (POE).

- CTPAT processes 54% of all imports into the United States. Industry Partners in CTPAT experience decreased supply chain disruptions, reduced and expedited inspections, and decreased wait times at land border POEs.

Trade Compliance

Trade compliance refers to an importer's ability to meet regulatory requirements imposed by CBP and other government entities.

- CTPAT currently maintains the Importer Self Assessment (ISA) Program to allow approved members to ensure their own compliance with regulatory requirements.

- After the Trusted Trader Pilot assesses benefits, the office will transition existing ISA members to the Trade Compliance portion of CTPAT.

Increasing benefits for CBP and traders

Global Reach
CTPAT, Trade Compliance, PGAs and MRA and AEOs
Trusted traders receive facilitated benefits globally

Partnership
CTPAT, Trade Compliance and PGAs
Trusted traders receive benefits at partner government agencies

Compliance
CTPAT, Trade Compliance
Traders are ISA compliant and meet CTPAT security requirements

Security
CTPAT
Traders are members of CBP's voluntary supply chain security program

Non-participant in CTPAT
But consistently low risk importers and exporters

2

CTPAT Security

As a supply chain security program, CTPAT requires participants to adhere to Minimum Security Criteria (MSC) and in exchange participants within the three different tiers experience benefits throughout the import process.

Impetus for Creation

- Created in the aftermath of 9/11 in response to an ongoing threat

- Voluntary government-business program to build cooperative relationships that strengthen and improve overall international supply chain and US border security

- First worldwide supply chain security program

- Requires businesses to ensure the integrity of their security practices and verify the security guidelines of their business partners within the supply chain

CTPAT Tiers (Importers/Exporters)

- Tier 1—Certified Member
  - ✓ Risk Score reductions

- Tier 2—Validated Member
  - ✓ MSC have been met
  - ✓ Significant Risk Score reductions

- Tier 3—Validated Member
  - ✓ Security measures exceed MSC and best practices have been adopted
  - ✓ Most significant Risk Score reductions

Piece of the Puzzle

- CTPAT is part of a layered law enforcement strategy

CTPAT

National Targeting Center

NII Technology Automated Targeting System

Trade Security

24 Hour Trade Act

Container Security Initiative

Intelligence

Benefits

- Reduced number of CBP examinations

- Front of line inspections

- Shorter wait times at the border

- Assignment of a Supply Chain Security Specialist to the company

- Access to Free and Secure Trade (FAST) Lanes at land borders

- CTPAT web-based Portal system and a library of training materials

- Eligibility for other U.S. Government pilot programs

CTPAT Security – Impact Today

Since CTPAT was established in November 2001, the Program has increased supply chain security and improved the safety of cargo at all points along the international supply chain.

11,400+ Certified Partners

→ **200+ minimum standards for membership**

→ **Over 30,000 validations conducted**

→ **Validation site visits conducted in 109 countries**

→ **11 Mutual Recognition Arrangements**

CTPAT provides a variety of benefits to CBP that allow the Agency to more effectively carry out its mission:

Increased Security

- Seeks to decrease supply chain attacks that may disrupt the flow of international commerce and pose a national security or safety threat to domestic industry and the public.

Greater Efficiency

- 54.1% of all imports (by value) into the U.S. are CTPAT Certified, importers make up the bulk of members at 37% and by taking advantage of program benefits cargo moves more effectively into the U.S.

Shared Responsibility

- Promotes shared responsibility from the trade community
- Promotes coordination and taking a proactive stance with industry to increase supply chain security as a voluntary program

CTPAT Security – Application Process

CTPAT has established a rigorous application process for vetting candidates to the program in order to ensure security and compliance measures are met and followed.

CTPAT Application Process

Eligibility - - - - - **Certification** - - - - - **Validation** - - - - - **Verification** ▶

Eligibility
- Applicants must apply online via the CTPAT web portal
- Eligibility requirements must be met before applicant's company information is inputted

Certification
- Each applicant must complete a security profile
- CTPAT has to review and either approve or reject within 90 days

Validation
- If the security profile is approved, CTPAT must conduct on on-site validation within one year

Verification
- CTPAT must ensure applicant complies with the program's security criteria
- Utilize verification process to develop a strong working relationship with the applicant

CTPAT Validations & Verification

Initial Validation Process
- Validation of reported supply chain security and alignment to guidelines
- Performed within 1 year from certification for all CTPAT participants
- Every 1-2 years continue to review forms, sign-in sheets and checklists

Periodic Re-Validation
- Re-validation occurs every 3-4 years
- A re-verification report will be written and participants have 90 days to respond by updating their actions in the web portal
- Participants are required to assess the level of risk business partners bring into the supply chain, which can be based on the recommended Five Step Risk Assessment Process
- Failure to respond timely can result in suspension or removal from the program

Long-Term Expectations
- Failure to show procedures are being followed can jeopardize future re-validation
- Expect to see improved procedures the longer participants are a member
- More stringent on requirements than original validation

CTPAT Security – Application Process

CTPAT has established a rigorous application process for vetting candidates to the program in order to ensure security and compliance measures are met and followed.

CTPAT Certification Process

📖 Certification

- During the certification process the assigned Supply Chain Security Specialist (SCSS) must vet all applicants prior to reviewing the security profile.
- Vetting thresholds have been established that cover any violations that a company may have been involved in.
- Vetting covers:
  - Terrorism
  - Narcotics
  - Human smuggling/trafficking
  - Money Laundering
  - Trade Violations
  - Other government agency violations
  - Other violations as deemed appropriate
- All CTPAT members are vetted annually, or more frequent if needed
- All vetting is documented

CTPAT Security – Current Minimum Security Criteria

U.S. Customs and Border Protection

The MSC are layered, cross-departmental security standards co-created by CBP and the trade community and spread across eight categories applicable to thirteen business entity types.

Minimum Security Criteria

I. Business Partner Security Requirements

Requires that Members to select, screen, and monitor their business partners' compliances with MSC.

II. Physical Access Controls

Requires the positive identification of all employees, visitors, and vendors at all points of entry.

III. Information Technology Security

Requires documented policies for user ID, passwords, email, internet access, hardware & software security.

IV. Personnel Security

Requires employees and contractors to complete screening, pre-employment verification, background checks, and comply with U.S. immigration laws.

V. Procedural Security

Requires Members to document processes relevant to transportation, handling, and storage of cargo.

VI. Security Training and Threat Awareness

Requires specific trainings to ensure that employees are able to identify, prevent, and respond to a security threat.

VII. Physical Security

Requires Members to deny unauthorized access to facilities and protect personnel and property via surveillance guidance.

VIII. Container Security

Requires a 7-point inspection on all empty containers and storage with a specific documentation by a qualified employee.

Applicable MSC Entity Groups

A core set of requirements across the 8 MSC Criteria apply to all partners, but custom criteria also apply to the 12 entity groups. Partners must adhere to all core and custom criteria.

- Air Carriers
- Consolidators
- Highway Carriers
- Foreign Manufacturers
- Marine Port Authority & Terminal Operators
- Rail Carriers
- Customs Brokers
- Exporters
- Importers
- Long Haul Carriers
- Sea Carriers
- Third Party Logistics Providers (3PLs)