



FOOTWEAR TRADE DISTRIBUTION & CUSTOMS

FTDC 2018 CONFERENCE

October 21–23 | The Renaissance | Long Beach

Critical Footwear Customs Updates with CBP

General Center Updates, Enforcement Within the AFT, C-TPAT, In-bonds, and More

James Snider

Assistant Director, Apparel, Footwear & Textile (AFT) Center, CBP

Crystal Morgan, *Supervisory Import Specialist, CBP*

Wayne Hooper, *Supervisory CBP Officer, CBP*

Department of Homeland Security ★ Customs and Border Protection



U.S. Customs and
Border Protection

Center Mission Statement

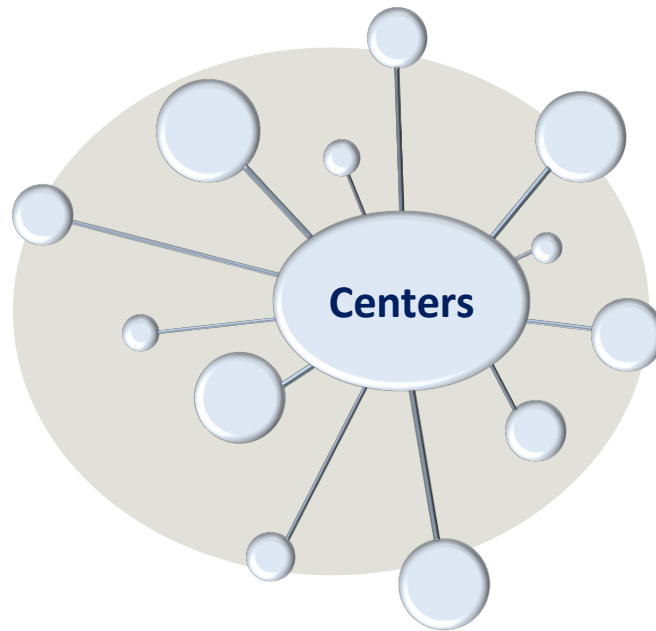
The Centers of Excellence and Expertise strengthen America's economic competitiveness and security through integrated industry knowledge and expertise, innovative trade processing procedures and trend analysis, global collaboration, and strategic and impactful trade enforcement actions.

The Centers:

- Strategically process post-release trade activities within industry sectors on a national basis
- Focus on industry-specific efficiencies to facilitate trade, reduce transaction costs, and increase uniformity and consistency
- Serve as an industry-focused resource for the public and private sectors
- Assess trade risks on an account and industry-wide basis to increase compliance with import laws, protect the American public and economy, and enhance the effectiveness of enforcement efforts



What are Centers of Excellence and Expertise?



- **Industry-focused** and **account-based** operational organizations processing post-release trade activities
- Aligned by 10 key industry sectors in strategic locations
- Consolidate existing expertise and build industry-specific education to authoritatively facilitate trade
- Provide national overview of accounts (importers) to identify areas for further facilitation or corrective action
- Serve as a resource to the broader trade community and to CBP's U.S. government partners

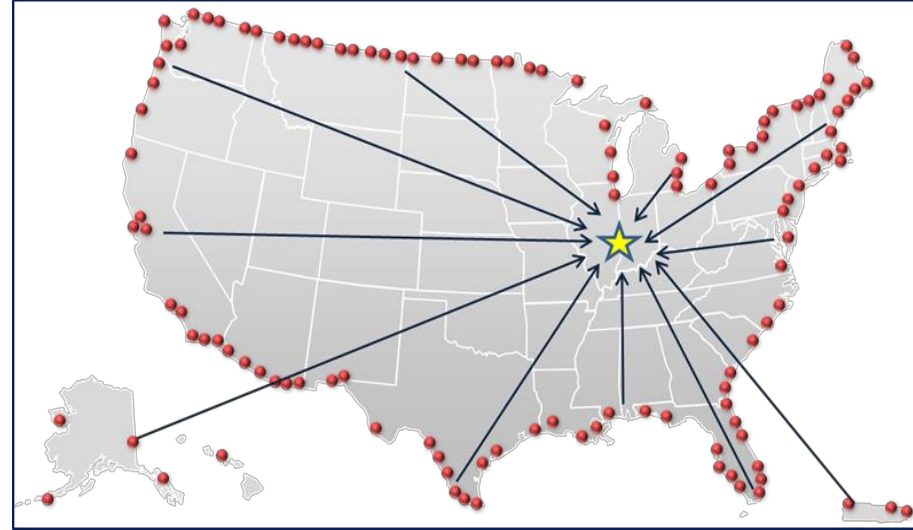
Centers are integrated into every facet of the trade process; from pre-arrival to final liquidation



U.S. Customs and
Border Protection

Why Centers?

- Objective:
 - Focus on industry-specific issues
 - Facilitation
 - Reduce transaction costs
 - Increase compliance
 - Increase uniformity of treatment
- Past processing:
 - Company imports into 60 ports of entry
 - 60 ports conduct entry summary reviews



- Centers
 - Company imports into 60 ports of entry
 - Single Center conducts entry summary reviews



Centers of Excellence and Expertise



U.S. Customs and
Border Protection

Goals of Centers

1. Increase industry-based knowledge within CBP
 - Advance cross-education to raise industry knowledge
 - Engage industry groups and key stakeholders
 - Identify industry trends and commercial threats
2. Facilitate legitimate trade through effective risk segmentation
 - Utilize account based methods to process trade
 - Expand partnerships - move more importers to trusted trader status
 - Develop and implement comprehensive strategies to manage risk
3. Enhance enforcement and address industry risks
 - Leverage industry to identify issues of mutual interest to provide CBP with targeting, enforcement, and/or intelligence information
 - Coordinate enforcement efforts by industry to address unique risks



Center Divisions

- Partnership Division
 - Contains multidisciplinary teams that process the trusted trader accounts and engage in cross-education efforts with the industry community.
- Validation and Compliance Division
 - Includes multiple Import Specialist teams and separate entry teams that process importers within the industry and applying risk segmentation schemes.
- Enforcement Division
 - Multidisciplinary teams that handle enforcement issues for the industry and develop strategic operations (i.e. trademark, patent, health and safety, ADCVD)



U.S. Customs and
Border Protection

Center Staff

- Centers staffed with existing trade and revenue positions
 - Assistant Center Directors
 - National Account Managers
 - Import Specialists
 - Entry Specialists
- Employees remain in their physical location at the Ports of Entry and work for a Center
 - Center chain of command
 - Multi-disciplinary teams across the nation



U.S. Customs and
Border Protection

Regulatory Authorities

- 19 CFR amendments effective Jan. 19, 2017
 - Interim Final Rule Issued December 20, 2016
 - Provides Center Directors with full authority to make trade decisions
 - Defines Centers and describes account based processing
 - Sets process for importers to appeal their Center assignment



U.S. Customs and
Border Protection

Regulatory Trade Authorities

Ports

- Cargo Release
- Manifest Processing
- Cargo Holds and Examinations
- Cargo Movement (permit to transfer, inbond)
- Export Compliance
- Seizures and Penalties
- Agriculture Exams
- Bonded Movements, Bonded Warehouses, and Foreign Trade Zones
- Narcotics, Anti-Terrorism and Security Risks
- Importer Security Filing Review

Centers

- Trade Admissibility Advice
- Entry Summary Reviews
- Free Trade Agreement Eligibility Review
- ADCVD
- Protests and Petitions
- Appraisals
- Post Summary Correction and Post Entry Adjustment
- CEAR Process
- Prior Disclosure Review
- Internal Advice
- Quota Processing

Centers and Ports collaborate on trade admissibility, decisions and determinations



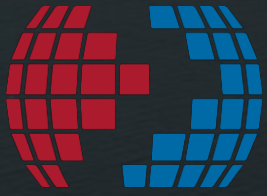
**U.S. Customs and
Border Protection**



U.S. Customs and Border Protection



U.S. Customs and
Border Protection



CTPAT

YOUR SUPPLY CHAIN'S STRONGEST LINK.

MSC UPDATE WORKSHOP

BUILDING ON THE PAST,
INNOVATING FOR THE FUTURE

AUGUST-OCTOBER 2018



U.S. Customs and
Border Protection

Introduction



Objective

- Provide background to the current update
 - Go over criteria categories, and provide context on why each was updated and what has changed
 - Work in teams and report on criteria/issues of concern
-

Flow of Workshop

1. Program Update
 2. Why we are updating the MSC and the process taken to strengthen it
 3. Requirement category deep dive
 4. Implementation timeline and expectations of CTPAT members
-

Feedback

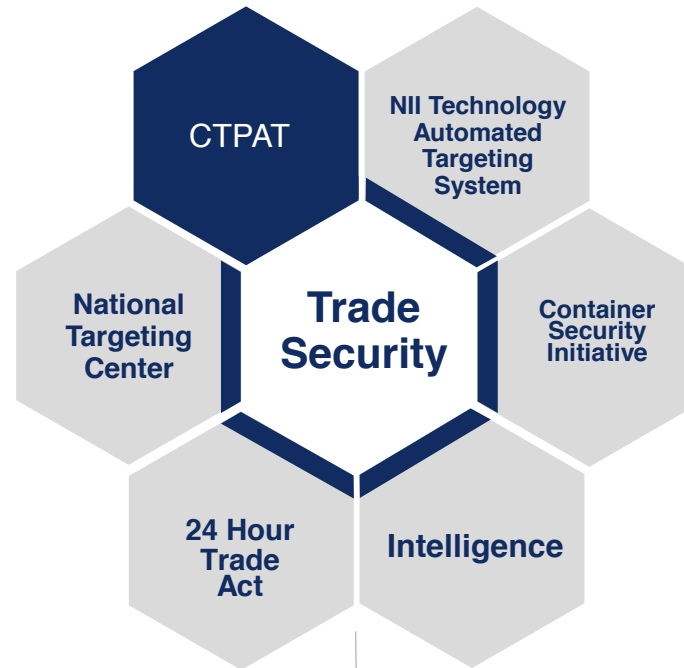
- To review the requirements in depth, utilize the entity specific MSC Workbooks that are posted on the CTPAT Portal
- Online feedback form is available on the CTPAT Portal
- If you still have questions or feedback following the workshop, please submit using this tool

CTPAT Program: Background and Update



Piece of the Puzzle

CTPAT is part of a layered law enforcement strategy



WCO Safe Framework

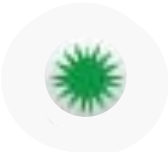


WORLD CUSTOMS ORGANIZATION

CBP Cargo Responsibilities



Updated CTPAT Eligibility Requirements



New: Maintain no evidence of financial debt to CBP for which the responsible party has exhausted all administrative and judicial remedies for relief, a final judgment or administrative disposition has been rendered, and the final bill or debt remains unpaid at the time of the initial application or annual renewal.

MSC Entity Groups

The 11,000+ members consist of companies across 12 entity groups. CTPAT members must meet Minimum Security Criteria (MSC) seeking to increase supply chain security.



857 U.S. Customs Brokers



357 Exporters



38 Air Carriers



869 Consolidators



2,946
Highway Carriers



4,139 Importers



430 Mexican Long
Haul Carriers



78 Sea
Carriers



1,682 Foreign
Manufacturers



11 Rail Carriers

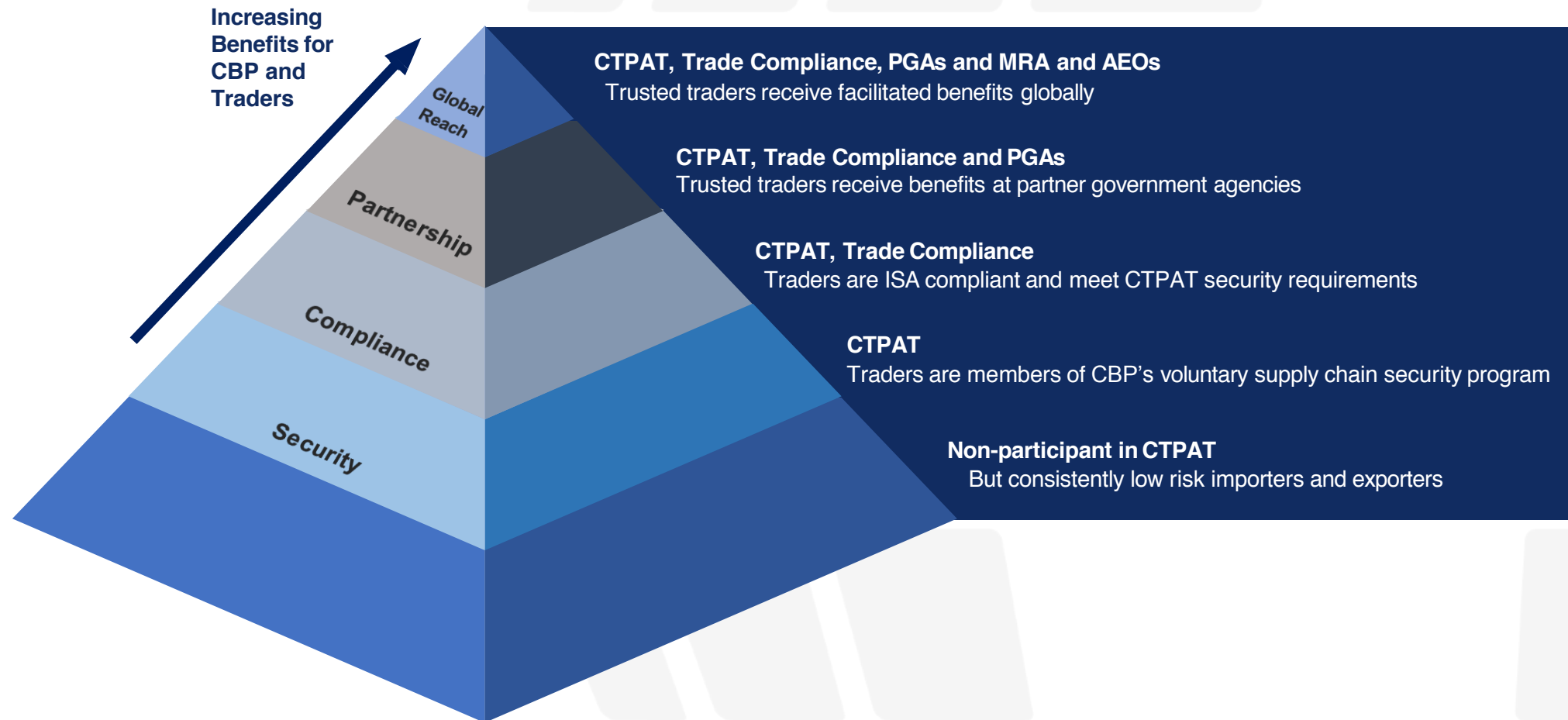


66 Marine Port
Authority & Terminal
Operators



111 Third Party
Logistics Providers
(3PLs)

CTPAT Program: COAC Trusted Trader Strategy



Strengthening the MSC

CTPAT's first major revision of the MSC since the program's inception modernized and strengthened requirements in order to more effectively combat evolving supply chain security threats.

Legal Mandates

The SAFE Port Act of 2006 includes reviewing and updating the MSC in consultation with the Trade.

The CTPAT Reauthorization Bill (HR 3551), currently in Congress, requires an annual review and subsequent revisions of the MSC.

Reflect CBP's Mission

Since 2003, when CBP was reorganized under the Department of Homeland Security (DHS), requirements have been both added and strengthened to reflect the evolution of the mission.

Changing Trade Landscape

Since CTPAT's inception, trade volume and complexity have increased exponentially. U.S. imports grew 88 percent from 2002 to 2016. The role of technology has increasingly impacted the supply chain.

The risk of data breaches and cyberattacks is more prevalent, creating the need for comprehensive cybersecurity.

CTPAT's Experience

The new MSC reflects the knowledge accumulated over years of working with our Partners via validations, conducting over 30,000 after action analysis to determine weaknesses, through industry collaboration, holding partner conferences and training seminars.

Terrorism and Criminal Activity

The global supply chain continues to be targeted by terrorists and criminal organizations, underscoring the need for CTPAT Members to take increased measures to secure their supply chains.

MSC Refinement and Restructure

Following multiple webinars, in-person reviews, and collaboration with the working groups, CTPAT has strengthened the MSC to enhance understanding and organization of the requirements.

New Focus Areas & Criteria Categories

Established **3 focus areas**, inclusive of **three new criteria categories** focused on Cybersecurity, Security Vision and Responsibility, and Agricultural Security

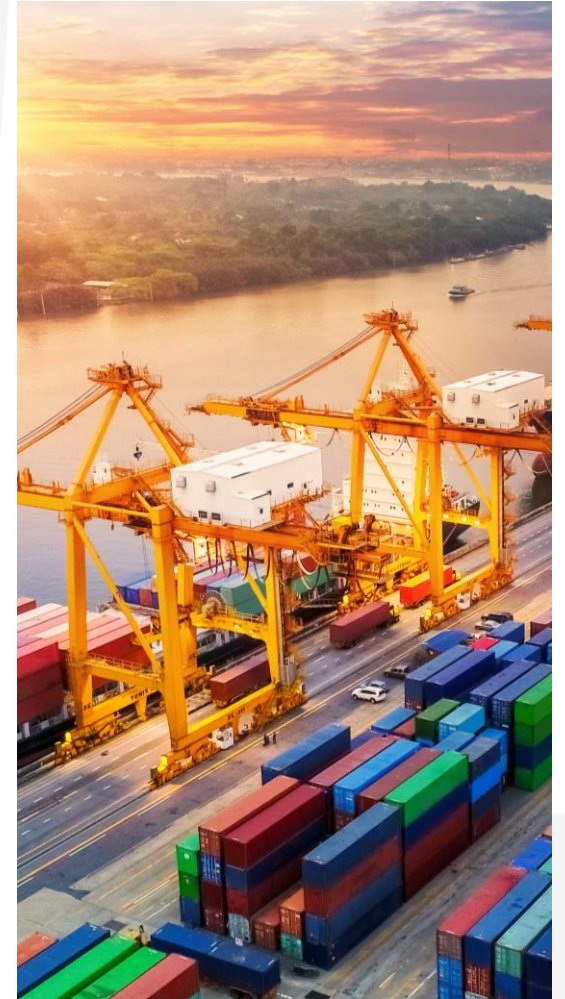
Must vs Should Requirements

Clarified language to explicitly organize requirements into **"Must" and "Should"** delineations (i.e. hard vs. soft) requirements across applicable entity groups based on risk

Mitigation of Modern Threats

Provided guidance regarding how to **combat Terrorism Financing and Money Laundering**, addressing a major threat in supply chain security

The process to update the MSC laid the groundwork for the modernization of criteria in order to combat today's threats in supply chain security



MSC Revision Summary

The following focus areas and criteria categories represent a holistic overview of the revised MSC requirements.

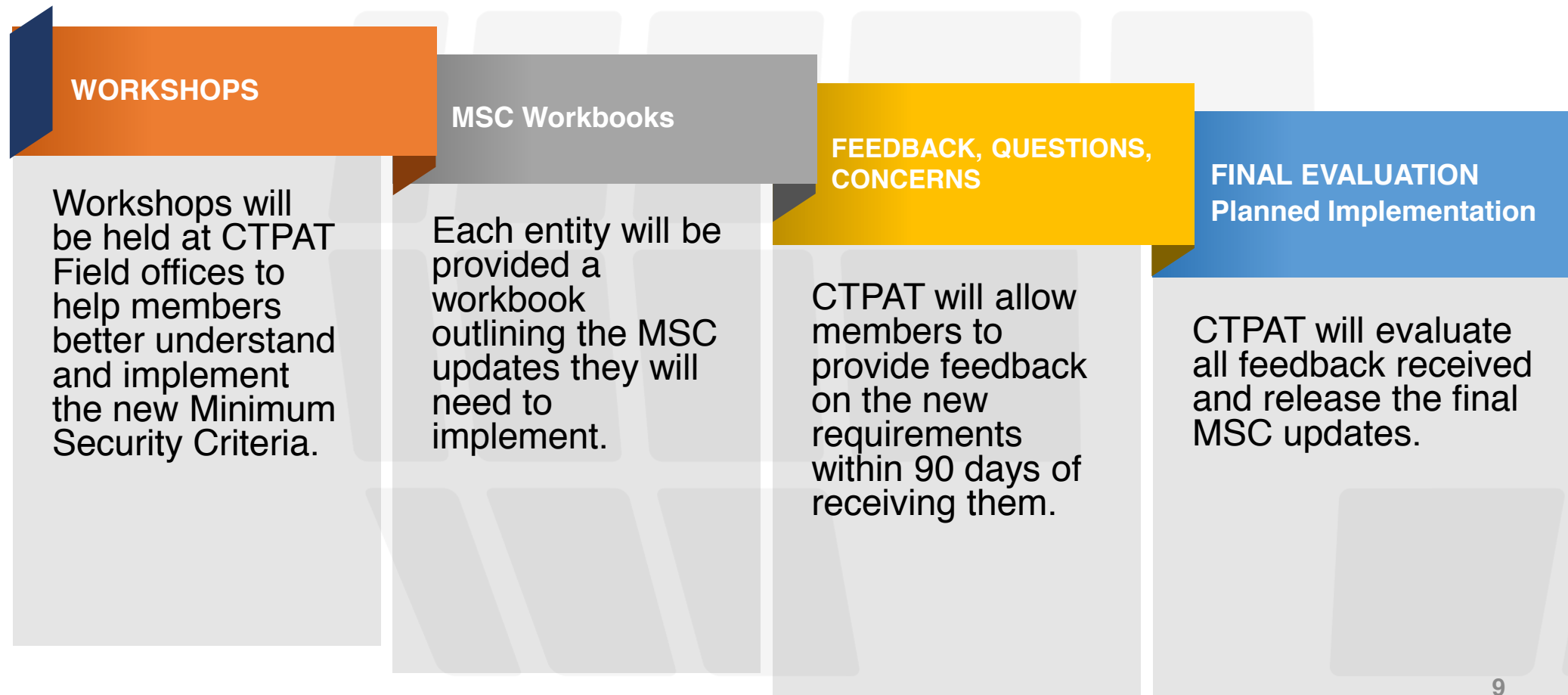


Focus Areas	Criteria Categories	Description
Corporate Security	Security Vision and Responsibility (New)	Promote a security vision, integrate security throughout the organization, establish an audit process, importance and role of the CTPAT POC
	Risk Assessment	Complete a comprehensive risk assessment based on a recognized methodology and in line with the MSC.
	Business Partner Requirements	Select, screen, and monitor business partner compliance with MSC, to include trade based money laundering
	Cybersecurity (New)	Written cyber security policies and procedures; protection of IT systems with software and hardware; remote access; personal devices
Transportation Security	Conveyance and IIT Security	Conduct thorough inspections for both security and visible agricultural contamination; driver verification; tracking of conveyances; random searches;
	Seal Security	High security seal policy; containers not suitable for sealing; mandated use of the VVTT seal verification process; management audits of seals
	Procedural Security	Document processes relevant to transportation, handling, and storage of cargo.
	Agricultural Security (New)	Introduces requirements that protect the supply chain from contaminants and pests and the proper use of wood packaging materials.
People & Physical Security	Physical Access Controls	Outlines requirements to prevent, detect, or deter unauthorized personnel from gaining access to facilities. Expands on the use of security technology.
	Physical Security	Require the positive identification of all employees, visitors, and vendors at all points of entry.
	Personnel Security	Complete screening, pre-employment verification, background checks, and comply with U.S. immigration laws.
	Security Training, Threat, and Awareness	Requires training on security for all employees; specialized training for employees in sensitive positions; determine if training provided was effective

MSC Socialization: August -October



CTPAT started the socialization of the Minimum Security Criteria to current members in August and will accept feedback or questions on the proposed MSC through October 2018.



MSC Categories – Security Vision and Responsibility

New Category: Supply chain security must become an integral part of a company's culture and it must be incorporated into its core business processes.

Overview

This criteria highlights the important role that managers play in how their security posture is organized –and how security is imbedded into the company's daily functions. Managers play a crucial role in establishing and maintaining the company's security program.

Summary of Requirements

- Statement of support for supply chain security
- Security program should reflect a cross-functional team
- Written audit process of security requirements
- Identifying points of contact with knowledge of CTPAT and supply chain security

Security Vision and Responsibility

Risk Assessment

Business Partner Requirements

Cybersecurity

Corporate Security

Conveyance and IIT Security

Seal Security

Procedural Security

Agricultural Security

Transportation Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and Awareness

People & Physical Security

MSC Categories – Risk Assessment

Overview

Requirements aligned to risk assessments detail how members can complete a comprehensive risk assessment based on a recognized methodology aligned with the MSC. These requirements highlight how and why members need to both document and map the movement of their cargo.

Summary of Requirements

- A two part risk assessment to identify where vulnerabilities exist, including: Member's Self-Assessment and International Risk Assessment
- Site-specific vulnerabilities (e.g., third parties)
- International supply chain mapping
- Annual review and update
- Crisis management, business continuity, and security recovery plans

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Business Partner Requirements



Overview

Updates to the business partner requirements include emphasizing the importance of conducting business partner assessments and evaluations, and focusing on measures to deter and mitigate money laundering and terrorism financing activities.

Summary of Requirements

- Ensure business partners meet or exceed CTPAT's MSC
- Screening and monitoring risk based process in place
- Evidence of business partner CTPAT or AEO membership as proof of business partner compliance with MSC
- Self-assessment questionnaires requirements
- Require and document that security deficiencies have been corrected
- Recommend business partners update self-assessment regularly

Security Vision and Responsibility

Risk Assessment

Business Partner Requirements

Cybersecurity

Conveyance and IIT Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and Awareness

MSC Categories – Cybersecurity

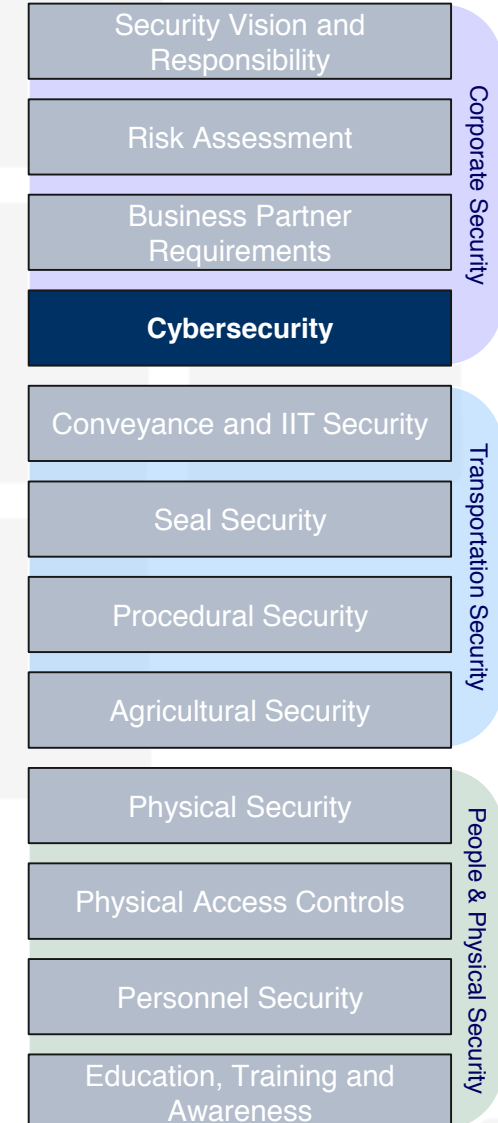
New Category: The cybersecurity criteria reflects the realities of a 21st century global economy –where data, and customer information move across cyberspace.

Overview

Technology has evolved dramatically since CTPAT's creation in 2001. A strong cybersecurity posture can better position CTPAT Members' organizations with business partners, customers, investors, and other stakeholders. The criteria in cybersecurity will help Members better deter cyberattacks and prevent loss of data.

Summary of Requirements

- Written policies and procedures
- Use of software/hardware to protect IT infrastructure
- Regular testing of the security of IT infrastructure
- Procedures designed to secure remote access from unauthorized users
- Review and update policies and procedures annually, or more frequently as circumstances dictate
- Measures to prevent the use of counterfeit or improperly licensed technological products
- Individually assigned accounts for individuals with access to information technology systems



MSC Categories – Conveyance and IIT Security



Overview

Conveyance and IIT security requirements detail procedures to conduct thorough inspections of IIT and maintain operational security requirements for driver verification and tracking. Conveyance and IIT security criteria are broken into cargo inspections, cargo tracking and highway carrier cargo security.

Summary of Requirements

- Procedures in place to verify integrity of conveyances and IIT
- Security and agricultural inspections prior to stuffing/loading
- Inspections should be conducted in an area of controlled access and under CCTV –if available.
- Record inspections on checklist
- Vacuum/wash conveyance/IIT if contamination found
- Periodic reviews by management of inspection processes
- Conveyances must be stored in secured areas
- Dispose personal garbage properly
- Sea Carriers – Pre-Departure Certificates for Asian Gypsy Moth

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

**Conveyance and IIT
Security**

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Seal Security

Overview

Requirements in the seal security category highlight the importance of using an ISO 17712 High Security seal; the proper sealing of containers; the role of management in conducting seal audits; and the mandated use of the VVTT seal verification process – a process already known to most of our Members. The sealing of tank containers and the security of shipments not suitable for sealing are also two issues addressed in this category.

Summary of Requirements

- Written high security seal procedures, reviewed no less than once a year
- Shipments must be sealed with a high security seal per ISO 17712 standard
- Digital photographs at point of loading/stuffing
- Procedures for recognizing and reporting compromised seals
- Periodic audits of stored seals
- Documented training for personnel that accept cargo containers and trailers
- Follow the VVTT process
- Procedures for seals control during transit / driver training
- Tank containers / Integrity of cargo not suitable for sealing

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Procedural Security



Overview

Requirements aligned to procedural security document processes relevant to transportation, handling, and storage of cargo.

Summary of Requirements

- Written process for auditing their security procedures
- Procedures for mitigating collusion between employees
- FAST lane requirements followed by all CTPAT drivers
- Highway carrier company using its own SCAC code when crossing the border
- Train personnel to review manifests and other documents in order to identify or recognize suspicious cargo shipments
- Procedures to prevent pest contamination and ensure compliance with WPM
- Maintenance program in place
- Procedures for reporting incident

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Agricultural Security

New Category: Invasive species cause over \$138B annually in economic and environmental losses. Eliminating contamination in conveyances and cargo may decrease holds, delays, and commodity returns and treatments.

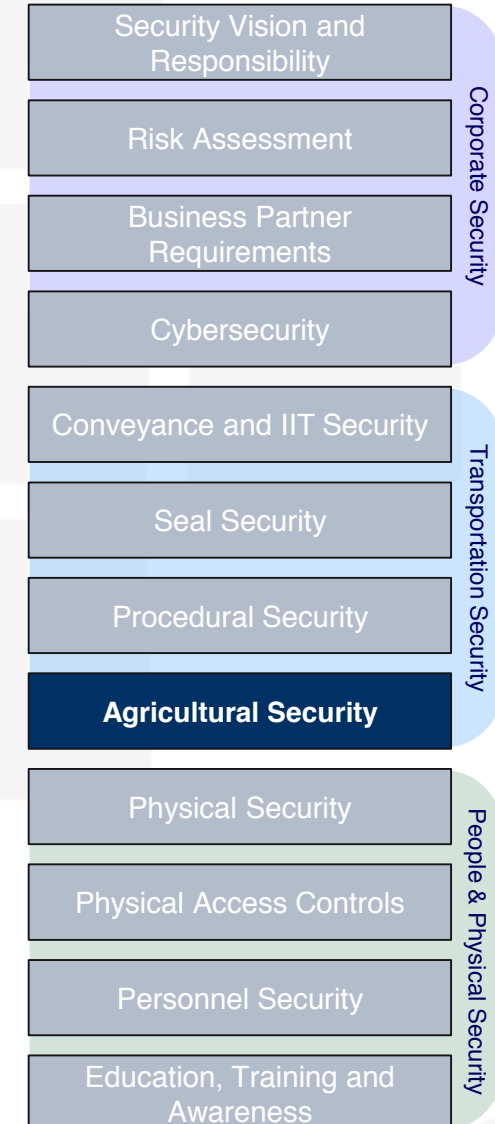
Overview

Agriculture security requirements are a critical addition to the program's criteria. While there is only one requirement in this category, it deals with two key issues: preventing pest contamination and compliance with Wood Packaging Materials.

Other criteria categories cover additional agricultural related requirements.

Summary of Requirements

- Procedures Designed to Prevent Pest Contamination
- Compliance with Wood Packaging Materials (WPM) Regulations



MSC Categories – Physical Security

Overview

The strengthened physical security criteria address the need to prevent unauthorized personnel from gaining access to building and facilities, and the expanded use of security technology.

Summary of Requirements

- Physical barriers and/or deterrents that prevent unauthorized access
- Restricted access to internal and external cargo handling areas
- Man or monitor functional gates where vehicles and/or personnel enter or exit and/or perimeter access points that can be closed and secured
- Position cameras to record key areas of facilities
- Maintain footage for a minimum of 14 days after the shipment being monitored has arrived at the point of destination
- Periodic, random reviews of the camera footage

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Physical Access Controls

Overview

Requirements aligned to physical access controls focus on the positive identification of all employees, visitors, and vendors at all points of entry along the supply chain.

Summary of Requirements

- Personnel identification system for positive identification and access control purposes
- Upon arrival, visitors, vendors and service providers present photo identification for documentation purposes
- Periodic screening of arriving packages and mail
- Procedures to identify, challenge and address unauthorized/unidentified persons
- Written work instructions and policies governing the work of security guards

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Personnel Security



Overview

Personnel security requirements are consistent with original MSC, and detail the need for members to complete employee screenings, pre-employment verifications, background checks, and comply with U.S. immigration laws.

Summary of Requirements

- Processes to screen prospective employees
- Verify application information prior to employment
- Conduct employee background screenings
- Written procedures governing how identification badges, facility, and access devices are granted, charged and removed

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

Education, Training and
Awareness

MSC Categories – Education, Training and Awareness



Overview

One of the key aspects of a security program is training. Personnel who understand why security measures are in place are more likely to adhere to them.

Summary of Requirements

- Establish and maintain training programs
- Additional specific training for sensitive positions
- Measures to verify that the training provided was effective
- Comprehensive security training includes measures to assist personnel in maintaining cargo and/or conveyance integrity
- Specialized training to personnel on warning indicators of trade based money laundering and terrorism financing
- Specialized training on preventing pest contamination
- Training on cybersecurity policies and procedures

Security Vision and
Responsibility

Risk Assessment

Business Partner
Requirements

Cybersecurity

Conveyance and IIT
Security

Seal Security

Procedural Security

Agricultural Security

Physical Security

Physical Access Controls

Personnel Security

**Education, Training and
Awareness**

Next Steps

Over the coming months, CTPAT Members will have the opportunity to review the revised MSC and provide feedback before the requirements are finalized



Provide Feedback

CTPAT asks that Members submit their feedback through the Portal's Feedback Form with actionable and specific recommendations for improvement



Review MSC Workbooks

Following this webinar presentation, CTPAT Members are encouraged to review the workbook relevant to their entity group, available on the Portal



CTPAT Conference

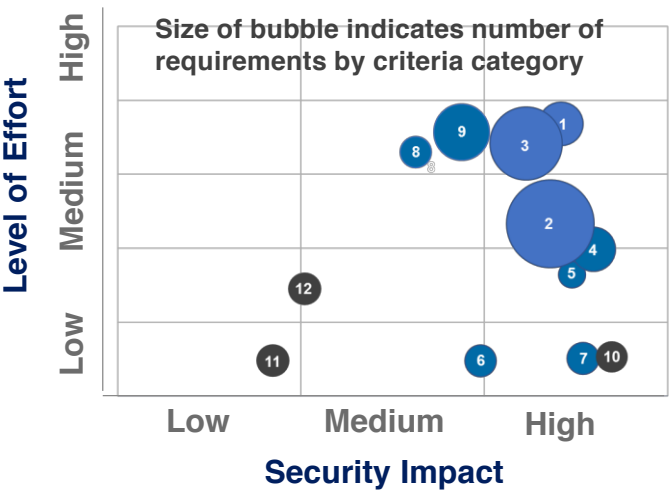
The annual CTPAT conference will be held in September 2018 and offer an opportunity for stakeholder training

CTPAT Security: Implementation Timeline



Based on guidance from the Trade and COAC, CTPAT is proposing the MSC to be implemented under a phased approach throughout 2019.

Notional Phased Implementation By Criteria Category:



Level of Effort

Measure of the cost, time, and reasonableness of compliance for CTPAT members.

Security Impact

Ability to address vulnerabilities in the supply chain and to complement existing legislative requirements or regulations.

Phase 01

- 1. Cybersecurity
- 2. Conveyance and IT Security
- 3. Seal Security

Phase 02

- 4. Security Training, Threat, and Awareness
- 5. Business Partner Requirements
- 6. Risk Assessment

Phase 03

- 7. Security, Vision, and Responsibility
- 8. Physical Security
- 9. Physical Access Security

Phase 04

- 10. Agricultural Security
- 11. Personnel Security
- 12. Procedural Security

Department of Homeland Security ★ Customs and Border Protection



U.S. Customs and
Border Protection



FEDERAL REGISTER

The Daily Journal of the United States Government



Rule

Changes to the In-Bond Process

A Rule by the [U.S. Customs and Border Protection](#) and the [Treasury Department](#) on 09/28/2017

PUBLISHED DOCUMENT

AGENCY:

U.S. Customs and Border Protection, Department of Homeland Security;
Department of the Treasury.

ACTION:

Final rule.

SUMMARY:

This final rule adopts, with several changes, proposed amendments to U.S. Customs and Border Protection (CBP) regulations regarding changes to the in-bond process published in the **Federal Register** on February 22, 2012. The in-bond process allows imported merchandise to be entered at one U.S. port of entry without appraisement or payment of duties and transported by a bonded carrier to another U.S. port of entry or other authorized destination provided all statutory and regulatory conditions are met. At the destination port, the merchandise is entered or exported. The changes in this rule, including the automation of the in-bond process, will enhance CBP's ability to regulate and track in-bond merchandise and ensure that in-bond merchandise is properly entered or exported. This document addresses comments received in response to the proposed rule and makes several changes in response to the comments that further simplify and facilitate the in-bond process.

DOCUMENT DETAILS

Printed version:

[PDF](#)

Publication Date:

[09/28/2017](#)

Agencies:

[U.S. Customs and Border
Protection](#)
[Department of the Treasury](#)

Dates:

This rule is effective on
[November 27, 2017](#).

Effective Date:

[11/27/2017](#)

Document Type:

Rule

Document Citation:

82 FR 45366

Page:

45366-45408 (43 pages)



U.S. Customs and
Border Protection

<https://www.federalregister.gov/documents/2017/09/28/2017-20495/changes-to-the-in-bond-process>

- * Except for merchandise transported by pipeline and truck shipments transiting the United States from Canada, the paper 7512 (Transportation Entry And Manifest Of Goods Subject To CBP Inspection and Permit) has been eliminated; henceforth carriers or their agents will be required to electronically file the in-bond application;
- * a standard 30-day maximum transit time to transport in-bond merchandise between U.S. ports will be in effect for all modes of transportation except pipeline and barge traffic. Movement by barge is 60 days
- * carriers will be required to electronically request and receive permission from CBP before diverting in-bond merchandise from its intended destination port to another port; and;
- * carriers will be required to report the arrival and location of the in-bond merchandise within 48 hours of arrival at the port of destination or port of exportation.
- * additional information on the in-bond application will include the six-digit Harmonized Tariff Schedule of the United States number if available.

<https://www.cbp.gov/border-security/ports-entry/cargo-control/bond/bond-regulatory-changes-faqs>



**U.S. Customs and
Border Protection**



U.S. Customs and Border Protection



U.S. Customs and
Border Protection