CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (CTPAT)

October 2021

U.S. Customs and Border Protection

CTPAT State of the Program

The Customs Trade Partnership Against Terrorism (CTPAT) is a partnership between Customs and Border Protection (CBP) and industry to **protect supply chains, identify security gaps, implement specific security and trade compliance best practices, and maintain the integrity of low-risk cargo** entering the United States.

Manuel A. Garza
Director, CTPAT
Office of Field Operations
U.S. Customs and Border Protection

RECENT ACCOMPLISHMENTS

Strengthening Supply Chain Security

Several recent narcotics seizures are a result of CTPAT partners informing their Supply Chain Security Specialist (SCSS) of supply chain anomalies, demonstrating the **powerful impact of strong partnerships between CBP and the Trade**

Prioritizing Social Compliance

CTPAT is developing **forced labor requirements** to be incorporated in FY21 as a part of CBP's Agency-wide efforts to combat the forced labor in global supply chains

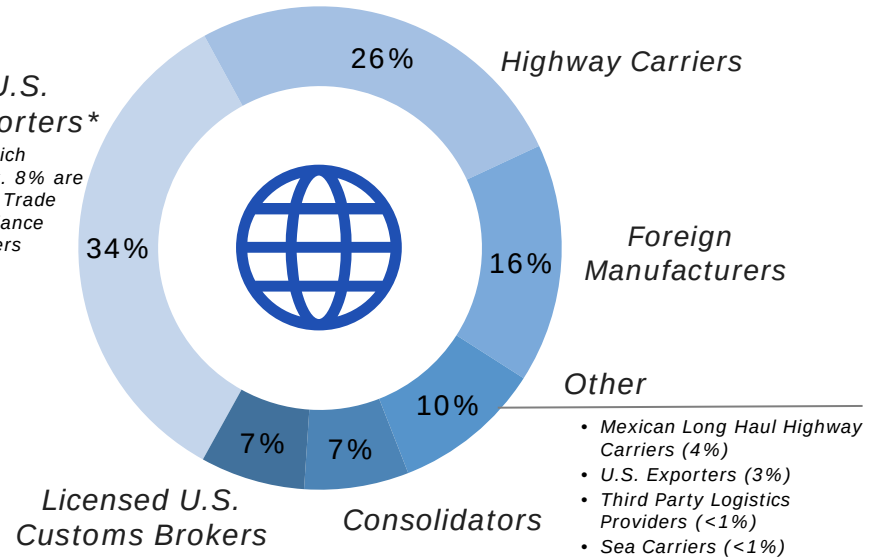
Collaborating with Global Partners

CTPAT works closely with its international counterparts through Mutual Recognition Arrangement (MRA) partnerships and the World Customs Organization (WCO) to further global standardization of supply chain security best practices. In January 2021, **the U.S. and the U.K. virtually signed an MRA**

CTPAT BY THE NUMBERS

11,100+	CTPAT Program Members
301	CTPAT Trade Compliance Members
234	CY20 Member Suspension & Removals
13	Mutual Recognition Arrangements
53%	Of U.S. Imports by Value are CTPAT Certified
90+	Speaking events in CY2020
99.5%	Compliance rate for C-TPAT members with the established CTPAT security guidelines
31.8M	Reduced examination cost savings benefit for C-TPAT trade members

CTPAT Entity Groups



CTPAT FY21 Priorities

In FY21, CTPAT will continue adapting operations to execute its mission during these unprecedented times while ensuring that its **partnership with Members remains strong and continues to set a high standard for global supply chain security and trade compliance.**

KEY FY21 PRIORITIES

Strengthen Global Supply Chain Security

*Advocate for global adoption of CTPAT's standards for end-to-end security to **address emerging threats across the global supply chain***

Rollout the Virtual Validations Process

*Leverage a risk-based approach that prioritizes Members eligible for the virtual validation process to **drive progress on the validation backlog***

Scale CTPAT Trade Compliance

*Finalize the Trade Compliance rollout that enables CTPAT to be a fully-fledged AEO Program to **ensure importer compliance with U.S. trade laws***

ADDITIONAL FY21 PRIORITIES

- Define CTPAT's approach to incorporate **E-Commerce** into the Program to advance CBP's E-Commerce Strategy and identify low-risk, e-commerce shipments
- Finalize and rollout **Forced Labor requirements** with OT and industry to support Member adoption of mitigation measures and enforce requirements
- Evaluate findings from the University of Houston Study on Program sentiment to identify areas to **implement advancements** to the Program
- Refine delivery and data collection process for **Member benefits** to enhance value to Members, process efficiency, and access to quantifiable metrics
- Update SAFE standards and AEO implementation guide with the **World Customs Organization** to strengthen global supply chain security

MSC Rollout & Security Profile Updates

MSC ROLLOUT

Enhanced MSC

To keep pace with an evolving threat environment, CTPAT continuously evaluates Program requirements and rolled out enhanced MSC in January 2020; notable updates include:

- ❖ New Agricultural Security Criteria Category
- ❖ Enhanced Cybersecurity Requirements
- ❖ Focus on Corporate Security Vision and Responsibility
- ❖ "Should" Criterion on Social Compliance Standards (Importers Only)

Training & Engagement

CTPAT continues to provide outreach to the trade community and develop guidance in support of the enhanced MSC and Program standards at large

- ✓ Participated in **93** speaking engagements throughout CY20
- ✓ Provided numerous **virtual trainings** to rollout the enhanced MSC
- ✓ Hosted a **three-day, Spanish language** session focused on new criteria

Validation Analytics

CTPAT has deployed a new data collection and analytic tool to support the MSC rollout, enabling CTPAT to:

1. Identify specific areas of the validation where partners had issues
2. Tailor training and outreach materials to support specific MSC
3. Capture historical data and compliance trends to inform future MSC updates

SECURITY PROFILE UPDATES

- ❖ CTPAT rolled out a **new security profile** on the CTPAT Portal on June 1, 2020, and provided guidance to Members to begin updating their profiles
- ❖ CTPAT has **reviewed and approved 5,769 of the 7,234 security profiles submitted by Members** through 1/26/2021
- ❖ CTPAT will consider **requests for 30-, 60-, 90- or 120-day extensions** on a case-by-case basis in coordination with the Members' SCSS

Virtual Validation Process Rollout

CURRENT VALIDATION PRIORITIES

- **Leverage advanced, secure technology** for virtual validations to reduce validation backlog
- **Continue to refine virtual validation process** that streamlines and automates actions for efficient validations
- **Demonstrate Member and Program compliance** through analysis of data captured during virtual validations
- **Reduce administrative burden** while maintaining rigor for CTPAT's validation process

SHORT-TERM EXPECTATIONS

Expectation	Description	Initial Actions
Comparative Analysis of Virtual Validation Pilot Data & Feedback	Advanced analysis of data and feedback obtained from the test virtual validations via WebEx to assess overall success compared to in-person validations and identify opportunities to **refine, standardize, and scale virtual validation and data collection processes**	• Collect data from a variety of sources including the validation worksheet, validation analytic tool, and interviews with CTPAT SCSSs for qualitative feedback • Define and track validation success metrics to assess any critical findings between data obtained in virtual and in-person validations
Virtual Validation Process Rollout & Trainings	HQ-facilitated trainings tailored for SCSSs and Members to introduce the new virtual validation process, including technology best practices, roles and responsibilities, and data and documentation submission, to **communicate and scale standard guidance for the virtual validation process**	• Document virtual validation process guidance for Field Offices, SCSSs, and Members informed by results of the virtual validation pilot analysis and the WCO • Develop a feedback mechanism that enables CTPAT to further a data-driven approach to assessing validation outcome and effectiveness

LONG-TERM EXPECTATIONS*

- **Secure Livestream Facility Tours and Member Interviews**
- **Intelligent Automation for Virtual Validation Processes**
- **Cognitive Analytics & Anomaly Detection for Virtual Validations**

**Currently in progress*

New MSC and Virtual Validation Findings - Brokers

Common Deficiencies Found

MSC ID	MSC Brief Description	Must/Should
2.1	Documented Risk Assessment to identify where security vulnerabilities exist, identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities	Must
3.1	Written, risk-based process for screening new business partners and for monitoring current partners	Must
2.4	Written procedures to address crisis management, business continuity, security recovery plans, and business resumption	Should
1.1	CTPAT statement of support signed by a senior company official and displayed in appropriate company locations	Should
8.1	Written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations	Must
12.1	Comprehensive, documented security training and awareness program that recognizes and fosters awareness of the security vulnerabilities at each point in the supply chain, which could be exploited by terrorists or contraband smugglers, and covers all CTPAT security requirements.	Must
1.3	Written review component where personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed	Must
12.6	Specialized, annual training to identify warning indicators of Trade-Based Money Laundering and Terrorism Financing	Should
4.1	Written cybersecurity policies and/or procedures to protect IT systems that cover all cybersecurity MSC	Must

New MSC and Virtual Validation Findings - Consolidators

Common Deficiencies Found

MSC ID	MSC Brief Description	Must/Should
2.1	Documented Risk Assessment to identify where security vulnerabilities exist, identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities	Must
3.1	Written, risk-based process for screening new business partners and for monitoring current partners	Must
8.1	Written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations	Should
1.1	CTPAT statement of support signed by a senior company official and displayed in appropriate company locations	Should
1.3	Written review component where personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed	Must
2.4	Written procedures to address crisis management, business continuity, security recovery plans, and business resumption	Must
12.1	Comprehensive, documented security training and awareness program that recognizes and fosters awareness of the security vulnerabilities at each point in the supply chain, which could be exploited by terrorists or contraband smugglers, and covers all CTPAT security requirements.	Must
4.1	Written cybersecurity policies and/or procedures to protect IT systems that cover all cybersecurity MSC	Should

Common Reasons for Deficiencies

- Inadequate evidence of implementation
- Failed to fully understand criterion
- Overall disregard for implementation
- Did not believe criterion was relevant to company

Virtual Validation Technology Issues

- Connectivity
- Noise echo
- Sound performance

Virtual Validation Preparation – Best Practices

Preparing for the Meeting

- Conduct internal audit
- Update Security Profile
- Timely communication
- Provide documents in advance
- Scan paper documents
- Reference MSC ID #(s)
- Test connection and meeting software
- Discuss any challenges

During the Meeting

- Appropriate personnel available
- Translator, if needed
- Free of distractions
- Articulate security processes
- Accessible evidence of implementation
- Share screens / documents
- Sharing sensitive information
- Virtual tour
- Take notes

Other Topics to Discuss

- Future of virtual validations
- Security in a remote work environment
- CTPAT Portal update
- How does CBP perceive CTPAT?
- Benefits
- What if I have issues?

Key Program Updates

UNIVERSITY OF HOUSTON PARTNERSHIP

STUDY GOALS

- Conduct informational assessment summarizing **perceptions** of CTPAT Program
- Evaluate Program to identify **challenges** and suggestions for improvement
- Identify cost-benefit **enhancements** for industry Members and the CTPAT Program
- Establish new and build upon existing Program **performance metrics**

PRELIMINARY FINDINGS

- **33%** of CTPAT Members participated in the survey
- **24%** of CTPAT Field Office Personnel were interviewed
- **Thousands of free text comments** from Members were received and analyzed as part of the survey
- **More than half of respondents** said CTPAT membership benefits outweigh the cost, which was measurably higher than the Program assessment from 2007

The final report was released in May 2021. CTPAT will evaluate the findings and begin implementation

CBP – SAT UNIFIED CARGO PROCESSING (UCP)

1 UCP PROOF OF CONCEPT

✓ Developed a proof of concept where CBP and SAT could jointly inspect cargo in the U.S. to streamline the processing of trusted partners cargo in Nogales, AZ

2016

2 PILOT AT MULTIPLE PORTS

✓ Worked with other ports of entry to pilot the process with trucks and quickly included rail cargo as the pilot proved successful at all locations: Land 15, Air 2; Rail 3

2016 - 2017

3 PROGRAM ROLLOUT

✓ Signed MOU on UCP and a Joint Statement on commitment to facilitate the secure flow of cross-border trade and reinforce our commitment to a “joint border management” approach

2017 - 2020

4 PROGRAM CONTINUATION

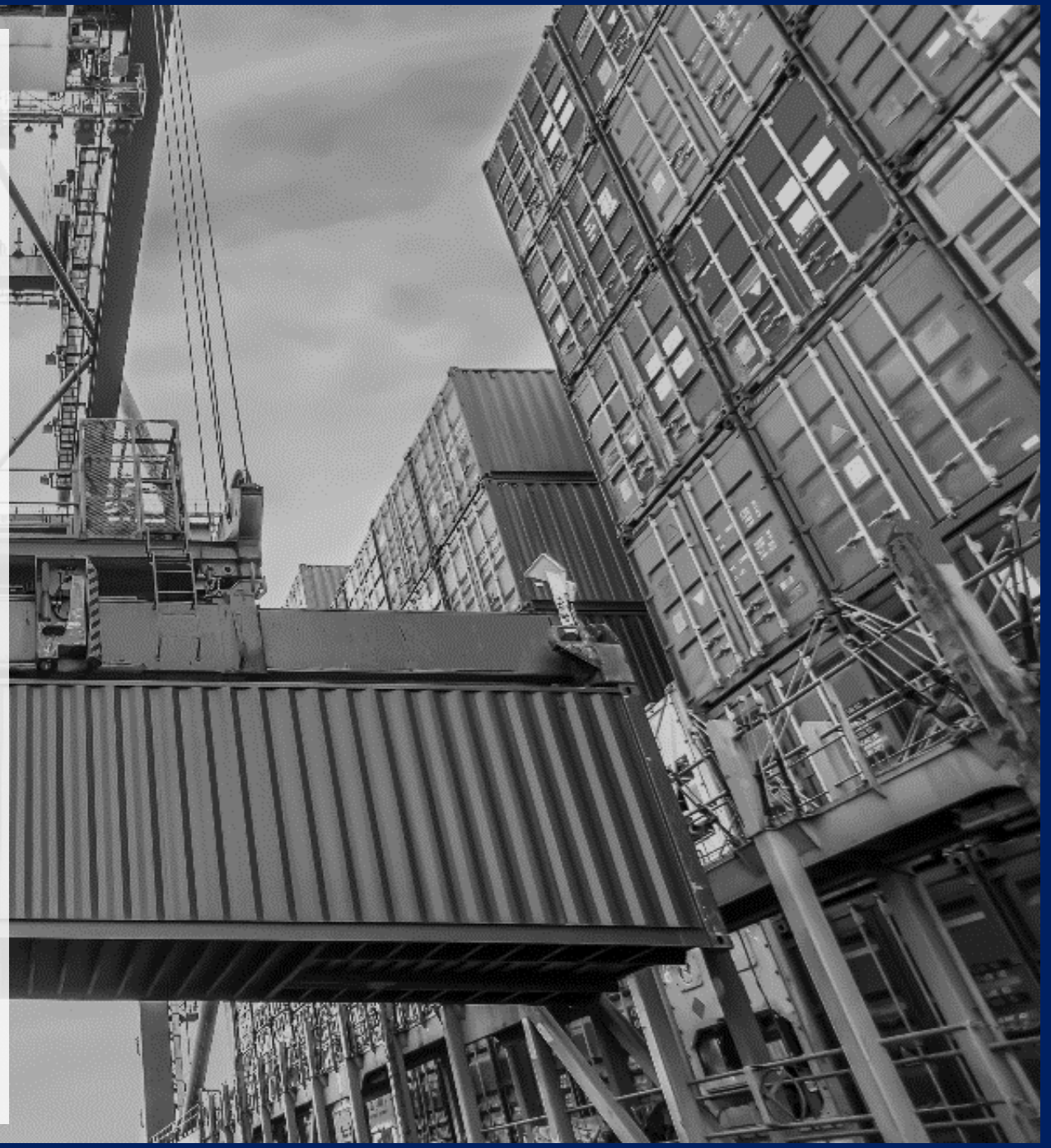
❑ Continue efforts to transition personnel to co-locations;
❑ Leverage co-locations for information sharing; and
❑ Streamline NII image sharing for both Customs administrations

2020 & Beyond

CTPAT Q&A

Adam Gunion
Supervisory Supply Chain Security Specialist

Los Angeles CTPAT Field Office
Office of Field Operations
U.S. Customs and Border Protection



CTPAT - Tips

1. **Communication is key to your success with the virtual meeting.**
   - If you don't know you don't know, do not assume. Many of the questions can be vague and require clarification.
   - Create a list of questions and collaborate with your Supply Chain Security Specialist to review and understand what is being asked and required.
   - Be sure that all members of your team are meeting regularly and are up to date on what is expected
2. **Create an Index sheet for all questions that have supporting documents uploaded into your CTPAT portal.**
   - All supporting documents need to list the document title, page number and section number where information specific to the question can be located. This provides a road map for your Supply Chain Security Specialist to easily verify details in the portal as well as for your team during the virtual meeting.
   - Each team member will be expected to share their screen and show supporting documentation when asked, your Index sheet will be a savior.
3. **Create a CTPAT Cross Functional Team document that lists the various individuals who will be on the call, be sure to provide their full name, title, and e-mail as well as a short bio of their responsibilities as they apply to the program. Examples would include:**
   - Compliance Personal
   - IT/Cyber Security
   - Human Resources
   - Training and Operations
   - Conveyance & ITT (Instruments of International traffic), Physical Security
   - Outreach / Marketing
4. **Security Team Roles**
5. Be sure all members of your Security team understand their role and have practiced what they are going to present each will be expected to speak individually on their expertise and responsibilities in your CTPAT program. It is very important that all members attending the call are well acquainted with using Teams especially screen sharing. Be yourself and try to make it a pleasant experience keep it simple and straight forward.