IMPORTERS

Minimum Security Criteria Update

July 2018

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

U.S. Customs and
Border Protection

IMPORTERS

Minimum Security Criteria Workbook for Importers

July 2018

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

U.S. Customs and
Border Protection

FOREWORD

I am pleased to present the Customs Trade Partnership Against Terrorism (CTPAT) *Minimum Security Criteria Workbook for Importers.* Created in partnership with industry, the new Minimum Security Criteria (MSC) advance the U.S. Customs and Border Protection (CBP) mission of securing the international supply chain.

The new MSC is the culmination of over 16 years of operational experience in supply chain security, including over 30,000 CTPAT validations and revalidations. Similar workbooks have been created for all business entities eligible for CTPAT Membership. The workbooks will be used as we continue to solicit input from our Membership prior to the ultimate implementation of the new requirements.

CBP aims to approach supply chain security comprehensively. To that end, CTPAT has incorporated requirements or recommendations related to cybersecurity, protection against agricultural contaminants, prevention of money laundering and terrorism financing, and the expansion of security technology. The proposed MSC maintain flexibility and a risk based approach, while redefining the global standard for government-led supply chain security programs.

This product is the result of the collaborative effort of the MSC Working Group (WG). In early 2016, CBP formally requested that the Commercial Customs Operations Advisory Committee (COAC) establish a working group to review and discuss CBP proposals for the MSC. The WG was created under the COAC's Global Supply Chain Subcommittee. The WG included half of the Members of the COAC, as well as individuals from several CTPAT companies, representatives from major trade organizations and associations, private sector supply chain security experts, CTPAT Supply Chain Security Specialists, and Headquarters program staff.

I would like to thank the private sector individuals from the WG – listed below – for their contributions. The WG was divided into six separate teams, with each team discussing a different set of criteria proposals.

Agricultural Security/Personnel Security Issues

Team A

Fermin Cuza – World Business Alliance for Secure Commerce – Team Lead
Brandon Fried – Air Freight Forwarders/COAC
Eugene Laney – DHL – CTPAT Consolidator
Alexandra Latham – COSTCO Wholesalers – CTPAT Tier III Importer/COAC
Dan Meylor – Carmichael – CTPAT Broker
Adam Salerno – U.S. Chamber of Commerce/COAC
Michael Young – Orient Overseas Container Line – CTPAT Sea Carrier/COAC

Cybersecurity

Team B

Bob Byrne /Alan Kohlscheen– IBM – CTPAT Tier III Importer/Exporter
Brandon Fried – Air Freight Forwarders/COAC
Alexandra Latham – COSTCO Wholesalers – CTPAT Tier III Importer/COAC
Adam Salerno – U.S. Chamber of Commerce/COAC
Lisa Schulte – Target Corporation – CTPAT Tier III Importer
Michael White – International Air Transportation Association/COAC
David Wilt – Xerox Corporation – CTPAT Tier III Importer – Team Lead
Michael Young – Orient Overseas Container Line – CTPAT Sea Carrier/COAC

Non-IT Security Technology

Team C

Barry Brandman – Danbee Investigations
Chuck Forsaith – Purdue Pharma – CTPAT Tier III Importer/
Foreign Manufacturer – Team Lead
Brandon Fried – Air Freight Forwarders/COAC
Alexandra Latham – COSTCO Wholesalers – CTPAT Tier III Importer/COAC
Liz Merritt – Airlines for America/COAC
Adam Salerno – U.S. Chamber of Commerce/COAC
Michael Young – Orient Overseas Container Line – CTPAT Sea Carrier/COAC

High Security Seals / Highway Carrier Issues

Team D

Dave Berry – Swift – CTPAT Highway Carrier/COAC
Ray Fernandez – Sealock Security Systems, Inc. – CTPAT Tier II Importer
Chuck Forsaith – Purdue Pharma– CTPAT Tier III Importer/Foreign Manufacturer
Alexandra Latham - COSTCO Wholesalers – CTPAT Tier III Importer/COAC
Kathy Neal – Regal Beloit Corporation – CTPAT Foreign Manufacturer –
Team Lead
Adam Salerno – U.S. Chamber of Commerce/COAC
Michael Young - Orient Overseas Container Line – CTPAT Sea Carrier/COAC

Prevention of Money Laundering and Terrorism Financing/Risk Assessment

Team E

Stella Bray-Conrad, David Blackorby, Theo Miles – Walmart Inc. –
CTPAT Tier III Importer/ Highway Carrier
Lisa Gelsomino – Avalon Risk Management/COAC
Alexandra Latham – COSTCO Wholesalers – CTPAT Tier III Importer/COAC
Kirsten A. Provence / Kathryn Gunderson – Boeing Company –
CTPAT Tier III Importer
Dan Purtell / Jim Yarbrough – British Standards Institute – Team Lead
Adam Salerno – U.S. Chamber of Commerce/COAC
Beverley Seif – Mohawk Global Trade Advisors – CTPAT Customs Broker
Michael Young – Orient Overseas Container Line – CTPAT Sea Carrier/COAC

Security Management and Administration

Team F

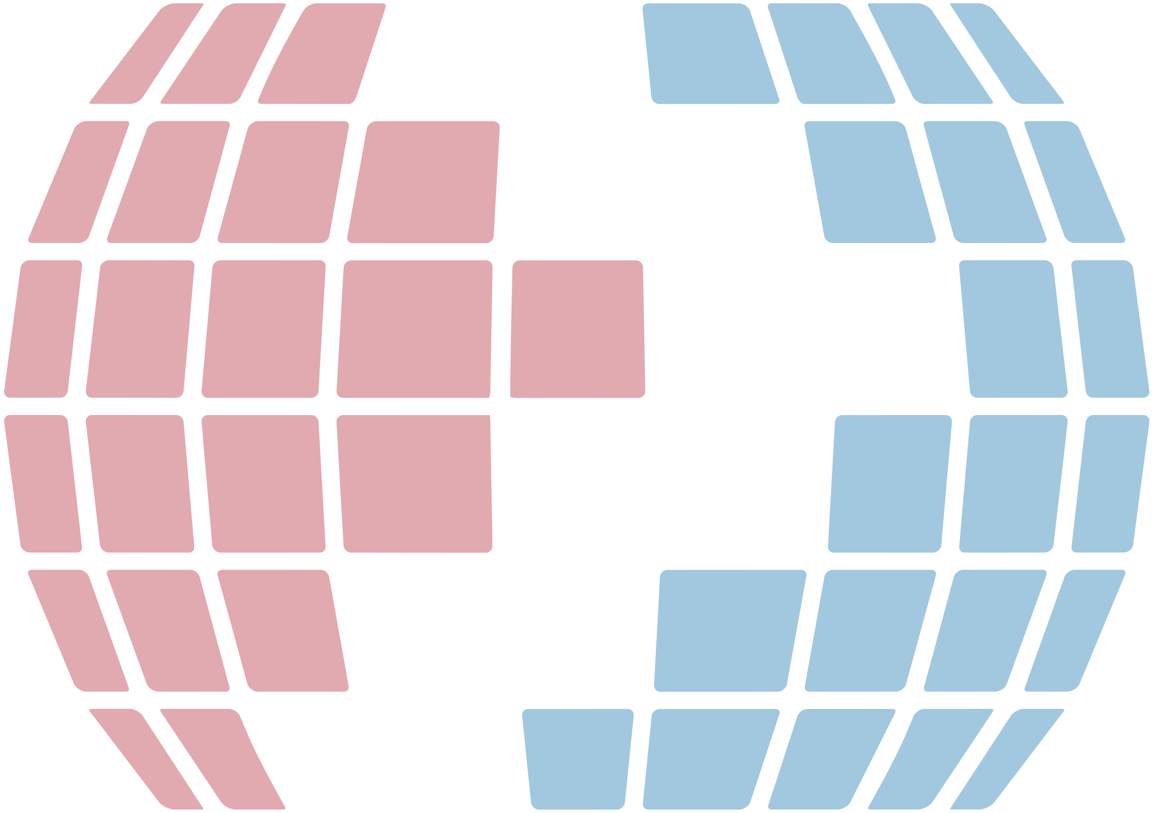
Barry Brandman – Danbee Investigations – Team Lead
Lana Dresen – S.C. Johnson and Son, SA De CV – CTPAT Foreign Manufacturer
Lenny Feldman – Sandler & Travis/COAC
Kevin J. Hayes – Long Beach Container Terminal/CTPAT Marine Port Terminal Operator
Vincent Iacopella – Alba Wheels Up – CTPAT Broker and Consolidator/COAC
Alexandra Latham – COSTCO Wholesalers – CTPAT Tier III Importer/COAC
Liz Merritt – Airlines for America /COAC
Adam Salerno – U.S. Chamber of Commerce/COAC
Doug Schneider – World Shipping Council
Michael Young – Orient Overseas Container Line – CTPAT Sea Carrier/COAC

Each of you are essential to the success of these requirements and are in a position to inform your colleagues and networks of our efforts to strengthen the international supply chain. We all reap the benefits of these shared efforts. Thank you for doing your part to protect our Nation and support CBP’s mission. I look forward to your input.

Sincerely,

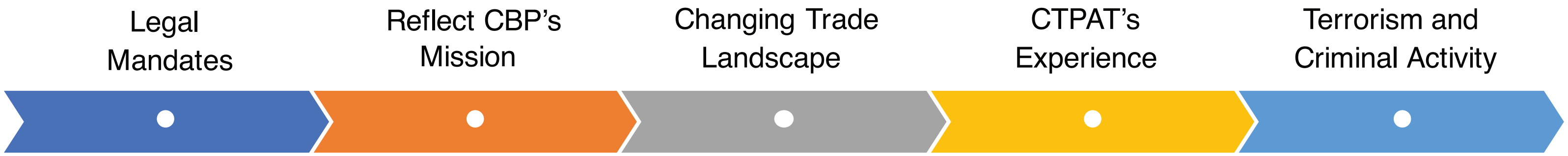
Todd C. Owen
Executive Assistant Commissioner
Office of Field Operations

TABLE OF CONTENTS



INTRODUCTION

The CTPAT program is a critical layer in CBP's multi-layered cargo enforcement strategy. Conceived shortly after the 9/11 attacks to protect our supply chains from terrorism, CTPAT is now one of the largest and most successful public-private sector partnerships in the world. CTPAT relies on its Partners to help strengthen supply chain security and improve U.S. border security. Since its establishment with just seven major Importers, the program has grown to over 11,500 Members, accounting for over 54% of the total value of U.S. imports.



Legal Mandates

Reflect CBP's Mission

Changing Trade Landscape

CTPAT's Experience

Terrorism and Criminal Activity

Case for Updating and Modernizing the Criteria

The present global trade environment faces new and evolving threats and challenges that the program needs to address. The current revision to the MSC reflects industry's valuable input, and responds to the following key factors:

Legal Mandates – The Security and Accountability for Every (SAFE) Port Act of 2006 codified the program and mandated strict timeframes for program requirements. The SAFE Port Act includes reviewing and, if necessary, updating the MSC in consultation with the Trade. Similarly, a CTPAT Reauthorization Bill (HR 3551), currently in Congress, requires an annual review and subsequent revisions of the MSC.

Reflect CBP's Mission – CTPAT was originally created under CBP's predecessor, the legacy U.S. Customs Service. In 2003, when CBP was reorganized under the Department of Homeland Security (DHS), the new agency inherited an expanded scope of responsibilities. As a result, 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, for example, grew 88 percent from 2002 to 2016. Simultaneously, 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 by CTPAT over years of working with our Partners via validations, conducting after action analysis to determine weaknesses, through industry collaboration, and 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. Cyberattacks or other types of data breaches continue to increase and all sizes and types of companies are at risk.

Principles Guiding the MSC Modernization

Principles guiding the MSC Modernization:

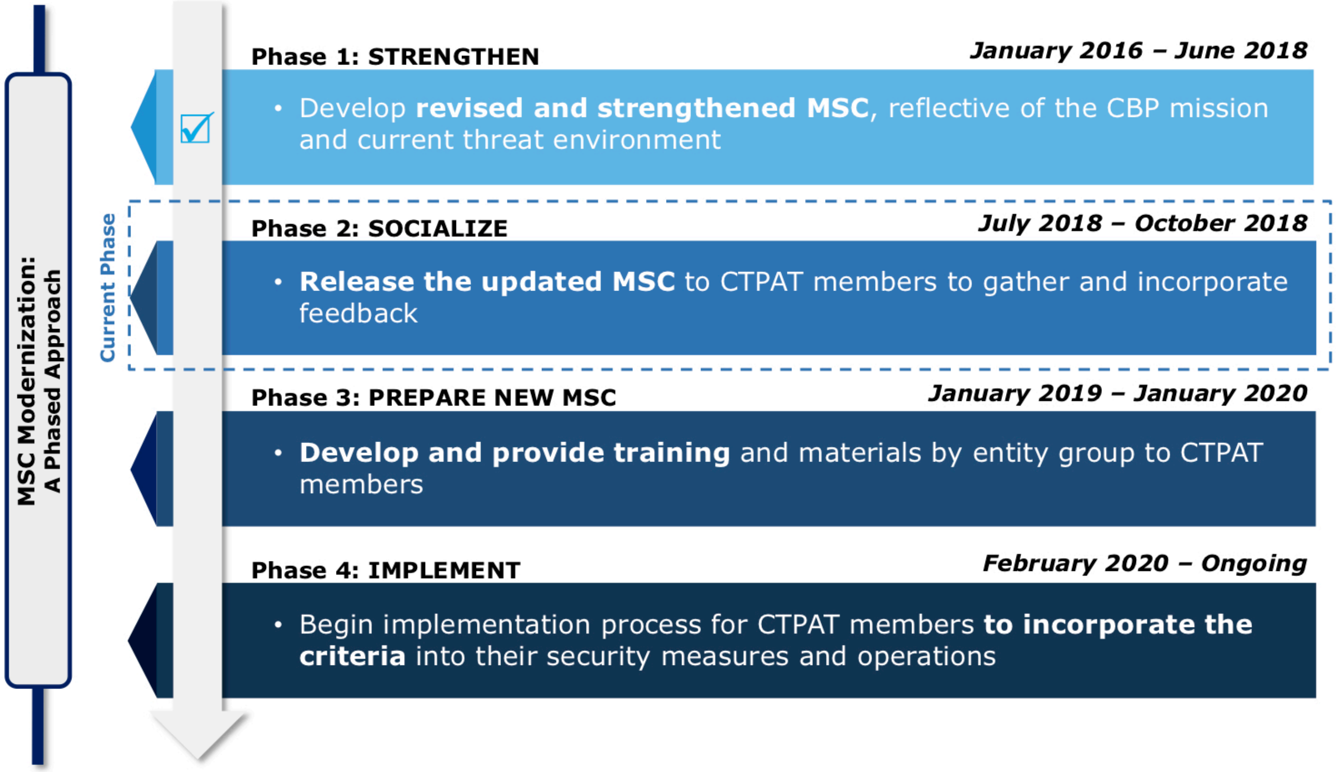
Partnership with the Trade – From the beginning of the process, CBP worked hand in hand with the COAC Global Supply Chain Subcommittee and other Trade partners to fully discuss and consider all perspectives and recommendations.

Bi-directional Education – CTPAT took into account the feedback from the Trade and wrote the updated draft of the MSC in plain language.

Consideration for Smaller Businesses – Any new requirements proposed and ultimately adopted by the program needed to be within the reach of small and medium-sized enterprises (SMEs).

Results Driven – New requirements needed to be logical, and proven to have a positive impact on the security of the supply chain.

To help track this process and facilitate the discussion, the program created a registry. The registry delineates all of the requirements, categorized by security impact and level of effort required by the company.



MSC Modernization: A Phased Approach

Current Phase

Phase 1: STRENGTHEN *January 2016 – June 2018*

☑

- Develop **revised and strengthened MSC**, reflective of the CBP mission and current threat environment

Phase 2: SOCIALIZE *July 2018 – October 2018*

- **Release the updated MSC** to CTPAT members to gather and incorporate feedback

Phase 3: PREPARE NEW MSC *January 2019 – January 2020*

- **Develop and provide training** and materials by entity group to CTPAT members

Phase 4: IMPLEMENT *February 2020 – Ongoing*

- Begin implementation process for CTPAT members **to incorporate the criteria** into their security measures and operations

CTPAT ELIGIBLE ENTITY GROUPS AND BENEFITS

Eligible Entity Groups

CTPAT Membership is open to 12 different business entities in the supply chain:

- Exporters
- Importers
- Foreign Manufacturers (Canada and Mexico)
- Mexican Long Haul Highway Carriers
- Air Carriers
- Rail Carriers
- Sea Carriers
- Highway Carriers (U.S./Canada and U.S./Mexico)
- Third Party Logistics Providers (3PL)
- Consolidators
- Marine Port Terminal Operators
- Customs Brokers

Member Benefits

Moving forward, CTPAT will encompass both supply chain security and trade compliance. Below are the benefits that apply to the respective Memberships.

SECURITY

CBP affords tangible trade facilitation benefits to CTPAT Members to recognize their demonstrated commitment to employ stronger security practices throughout their international supply chains. The value of CTPAT Membership goes beyond dollars and cents—it includes risk avoidance, a communal approach to a safer supply chain, the ability to compete for contracts that require CTPAT Membership, and the advantage of the credibility that CTPAT Membership affords. The CTPAT benefits package has increased over the years, and the program continues to explore additional benefits with the trade community. The current benefit package includes:

- **Assigned Supply Chain Security Specialist (SCSS):** Assigned SCSS who acts as an advisor to help the CTPAT Member improve and maintain its security posture.

- **Advanced Qualified Unlading Approval Pilot ("AQUA Lane"):** Expedited clearance of sea vessels through the AQUA Lane, creating cost savings of $3,252.75 per hour per vessel for low risk Sea Carriers.

- **Free and Secure Trade (FAST) Lanes:** Shorter wait times at the border and access to the FAST Lanes.
- **Front of the Line:** When feasible for ports, CTPAT shipments are moved ahead of any non-CTPAT shipments for exams. Front of the Line inspection privileges apply to screening by non-intrusive inspection equipment, examinations conducted dockside or at a centralized examination station, and all other inspections conducted for security, trade and/or agriculture purposes.
- **Reduced Examination Rates:** Reduced examination rates leading to decreased importation times and reduced costs.
- **Business Resumption:** Priority entrance of goods following a natural disaster or terrorist attack.
- **Mutual Recognition Arrangements (MRAs):** Expedited screening with worldwide security partners from a number of the foreign Customs administrations that have signed MRAs with the United States.
- **Training Seminars:** Access to CTPAT sponsored events such as CBP training seminars and the CTPAT Conference.
- **CTPAT Portal:** Access to the CTPAT web-based Portal system and a library of training materials.
- **Best Practices:** Access to CTPAT best practices through guides, catalogs, and training materials.
- **Status Verification Interface (SVI) Access:** SVI Access that includes the verification of companies yearly.
- **Security Validation:** As part of the validation or revalidation process, CTPAT Members receive a comprehensive evaluation by a government SCSS expert who assesses the Member’s security posture.
- **SAFETY Act:** The SAFETY Act of 2002 created liability limitations for claims resulting from an act of terrorism where Qualified Anti-Terrorism Technologies (QATTs) have been deployed. The Act applies to a broad range of technologies, including products, services, and software, or combinations thereof.

TRADE COMPLIANCE

Trade compliance refers to an Importer’s ability to meet regulatory requirements imposed by CBP and other government entities. To modernize trade compliance, CTPAT is currently executing the Trusted Trader Strategy, which is transitioning the current Importer Self-Assessment Program into the new CTPAT Trade Compliance program by the end of FY 2018. As part of this effort, CTPAT is working with Trade Compliance stakeholders to test over 30 benefits and measure their impact on industry. The ultimate goal is for Members to document their return on investment and quantify the value for their participation in the program. The transition of CTPAT Trade Compliance will create the United States equivalent of an Authorized Economic Operator (AEO) program, addressing both security and customs trade compliance.

- **National Account Manager:** Access to an assigned NAM, who acts as an advisor and liaison between CBP HQ and the CTPAT Trade Compliance Member.

- **Multiple Business Units:** Opportunity to apply for coverage of multiple business units.

- **Removal from Focused Assessments Pool:** Will be removed from the Regulatory Audit's (RA) audit pool established for Focused Assessments. However, Importers may be subject to a single issue audit to address a specific concern.

- **ITRAC Data Access:** Entitled to receive Importer Trade Activity (ITRAC) data free of charge.

- **CTPAT Trade Compliance Portal** *(In Development)***:** Access to the Trade Compliance section of the CTPAT Portal, and use of the CTPAT Portal to access and update information related to Trade Compliance in the new Portal component.

- **Reconciliation** *(In Development)***:** Ability to flag and un-flag entries for reconciliation after the entry summary is filed up to 60 days prior to the date for which liquidation of the underlying entry summary has been set.

- **Expedited Rulings** *(In Development)***:** Rulings and Internal requests will have priority and be placed at the front of the queue for processing within 20 days by the receiving office.

- **Release of Goods to Premises for Exam** *(In Development)***:** Importers who file an entry in ACE will receive a release message and be allowed to remove containers from the port under customs supervision to a facility of their choosing that contains accommodations CBP considers amenable for a thorough exam.

- **Exemption from Random NIIs** *(In Development)***:** Ability to "opt out" of this incentive entirely or identify the ports where the Member wants this incentive applied.

- **Confidential Manifest Automation** *(In Development)***:** Cargo manifest data as described under 19 CFR 103.31 will be kept confidential through automated means instead of having to manually request for this status every two years through a burdensome process.

- **ITRAC Data Automation** *(In Development)***:** ITRAC Data will be provided within the CTPAT Trade Compliance Portal, and Members will be provided with tools that allow for the evaluation of that data.

CTPAT SECURITY AND TRADE COMPLIANCE

The following benefits are available to both CTPAT Security and Trade Compliance Members:

- **Penalty Mitigation:** CBP FP&F will ensure that the company's Trusted Trader status is taken into consideration and that any penalties may be offset by the measure/level of the corrective actions taken to prevent future occurrence. A letter will indicate their Trusted Trader status and other pertinent information. Trusted Traders requesting a penalty offset will ensure that the cover letter to Fines Penalties & Forfeitures copies a NAM.

- **Marketability of CTPAT Membership:** Much like certification with other U.S. government agencies or the International Standards Organization (ISO), CTPAT Membership can raise a Member's reputation and ability to secure business.

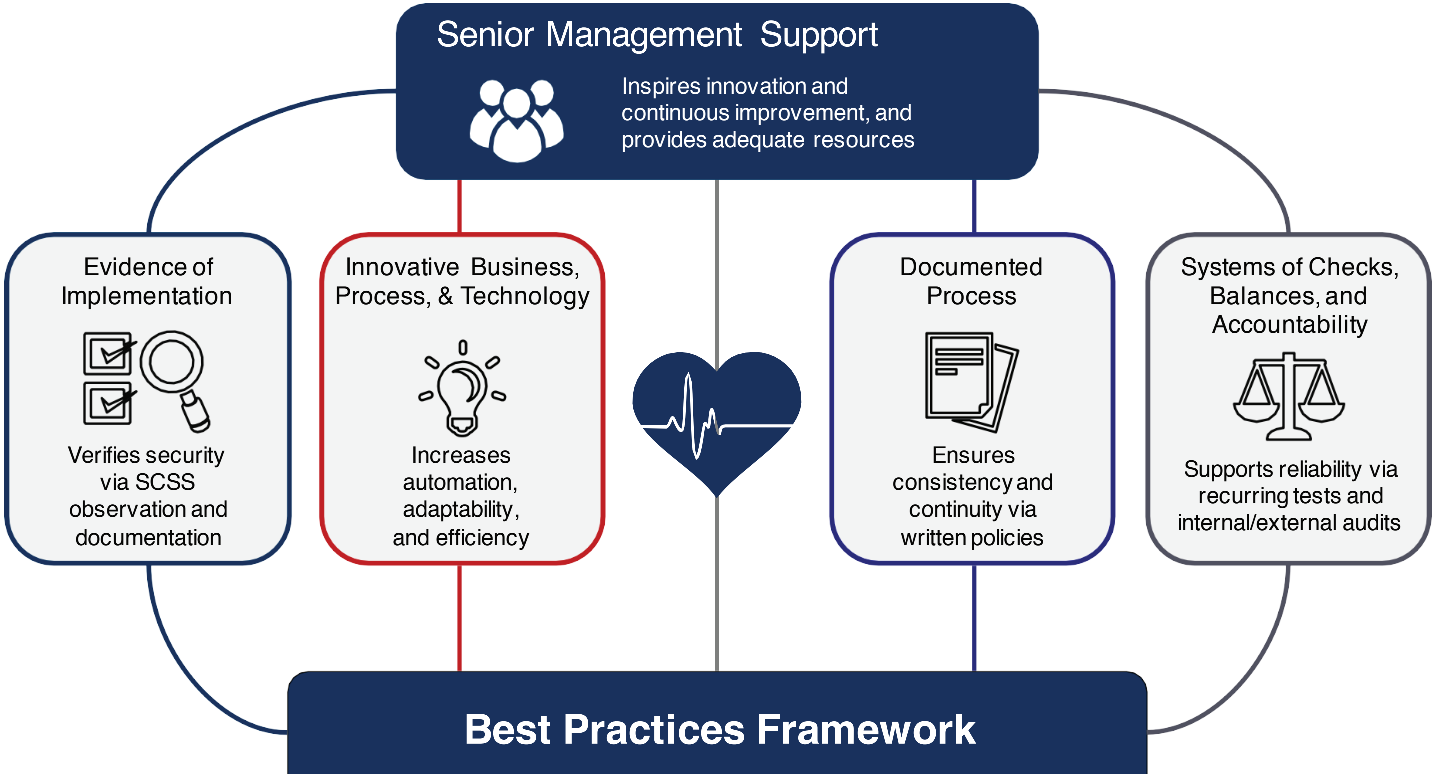
- **CTPAT Defender** *(In Development)***:** This identity theft benefit alerts Members if their Importer of Record (IOR) number is used for an entry that does not match a profile of identifying characteristics selected by the Member to reduce liability for fraudulent IOR use.

Best Practices

CTPAT Partners must exceed the Minimum Security Criteria (MSC) to achieve Tier Three status. Previously, Members exceeded the MSC by complying with specific lists of best practices that CBP published. After extensive dialogue with the trade community, CTPAT determined that this approach both did not provide clear guidance and also established best practices that quickly became industry standards.

The program, in consultation with the Trade, determined that a best practices framework created a more agile and effective process, since a framework – as opposed to a prescriptive list – allows companies to identify or build specific and unique best practices.
For CTPAT purposes, a best practice must meet all five of the following requirements, all of which are subject to verification: senior management support; innovative technology, process or procedures; documented process; verifiable evidence; and a regular system of checks, balances and accountability.

The best practices framework was tested and validated by COAC Minimum Security Criteria Working Group Members.



Senior Management Support

Inspires innovation and continuous improvement, and provides adequate resources

Evidence of Implementation

Verifies security via SCSS observation and documentation

Innovative Business, Process, & Technology

Increases automation, adaptability, and efficiency

Documented Process

Ensures consistency and continuity via written policies

Systems of Checks, Balances, and Accountability

Supports reliability via recurring tests and internal/external audits

Best Practices Framework

MINIMUM SECURITY CRITERIA OVERVIEW/ FOCUS AREAS

The new criteria takes a more comprehensive approach towards supply chain security. The new criteria includes new requirements - "musts" - and recommendations - "shoulds" - in the following areas:

- Cybersecurity
- Protecting the supply chain from agricultural contaminants
- Prevention of trade based money laundering and terrorist financing
- Use of security technology - including cameras and intrusion alarms

Other requirements, particularly those related to the security of cargo containers, as they move through the land border environment, have been strengthened. For instance, CTPAT added recommendations and requirements to mitigate the risk of collusion between employees, e.g., a driver and dispatch personnel.

The Working Group categorized the new criteria into three main focus areas: Corporate Security, People and Physical Security, and Transportation Security. Within these, there are 12 criteria categories that apply across the supply chain to each entity group.

CORPORATE SECURITY:

As part of the corporate security focus area, upper level management are held accountable to ensure the program is implemented in a sustainable manner. The Risk Assessment is now broadened to include a criterion on business continuity. The new criteria aim to increase accountability across departments by establishing a company wide culture of security, implementing a system of checks and balances, expanding cybersecurity protocols, and training personnel on supply chain security best practices.

TRANSPORTATION SECURITY:

The transportation security focus area relates primarily to the physical movement and handling of goods throughout the supply chain. The processes and procedures highlighted throughout these requirements cover familiar territory:

- Ensuring import and export processes follow security protocols and all paperwork is secured;
- Conducting inspections of instruments of international traffic (IIT) such as containers, trailers, and Unit Load Devices (ULDs);
- Complying with security seal protocols; and
- Maintaining operational security of cargo in transit.

New criteria in this focus area aim to prevent the contamination of IIT from agricultural pests. These procedures complement the existing security protocols.

PEOPLE AND PHYSICAL SECURITY:

The people and physical security group encompass well known criteria for securing facilities, screening, and training personnel. The education of employees is a key component of the criteria, and as such, the education has been expanded and is now a requirement. Criteria governing the use of security technology - such as security cameras and intrusion alarms - have been added or expanded, but are only applicable to companies utilizing this type of technology to secure their facilities. The Physical Security aspects of the criteria have always been based on the level of risk for a facility and/or supply chain, and that will continue to be the case.

Focus Areas	Criteria Categories
Corporate Security	Security Vision and Responsibility (New)
	Risk Assessment
	Business Partner Security
	Cybersecurity (New)
Transportation Security	Conveyance and Instruments of International Traffic Security
	Seal Security
	Procedural Security
	Agricultural Security (New)
People and Physical Security	Physical Access Controls
	Physical Security
	Personnel Security
	Education, Training, and Awareness

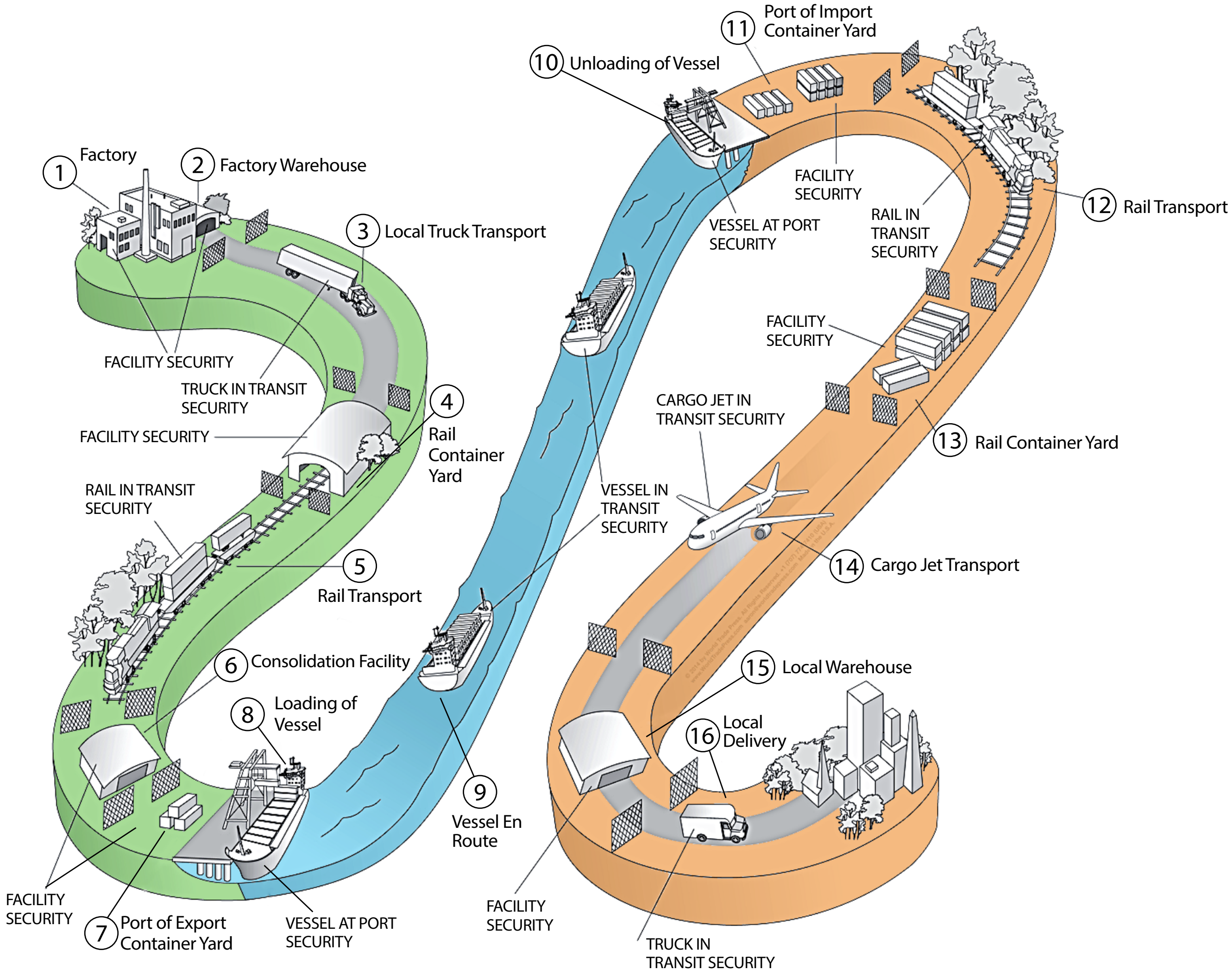
MINIMUM SECURITY CRITERIA FOR U.S. IMPORT PROCESS

Supply Chain Map

CTPAT recognizes the complexity of international supply chains and endorses the application of security measures based upon risk. The program allows for flexibility and the customization of security plans based on the Member's business model. Appropriate security measures, as listed throughout this document, must be implemented and maintained - based on risk - throughout the Member's supply chains.

CTPAT defines the supply chain as beginning at the point of origin - where cargo destined for export to the United States has been made, assembled, grown and/or packed for export - and ending at point of distribution in the United States.

CTPAT Members must ensure the security of their cargo at every point in their supply chain. The following map demonstrates potential locations where cargo could be compromised. Importantly, these are all locations where a validation site visit could take place to ensure that a Member or business partner is meeting the CTPAT security criteria.



Updated Eligibility Requirements

To qualify for CTPAT as an Importer, a company must meet the following requirements:

- Be an active U.S. Importer or Non-Resident Canadian Importer. Active is defined as having imported goods into the U.S. within the past 12 months.
- Have and maintain an active U.S. Importer of record (IOR) number in one of the following formats: U.S. Social Security Number, Internal Revenue Service assigned ID(s), or CBP assigned Importer ID.
- Have and maintain a valid continuous import bond registered with CBP and operate a business office staffed in the United States or Canada.
- Designate a company officer that will be the primary cargo security officer responsible for CTPAT.
- Demonstrate commitment to maintaining the CTPAT supply chain security criteria as outlined in the CTPAT Importer agreement.
- Complete a supply chain security profile populated in the CTPAT Portal, identifying how the Importer will meet, maintain, and enhance internal policy to meet the CTPAT Importer security criteria.

✳ 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.

Providing Feedback via the Online Feedback Form

To continue soliciting feedback from the Trade on the new MSC, CTPAT Members have the opportunity to provide input using the Feedback Form posted alongside this document in the CTPAT Portal Document Library. We ask that comments be objective, actionable, and specific in order to be considered. Each CTPAT Member will have the opportunity to submit one feedback form per organization.

Minimum Security Criteria by Category

a. Same, new, or strengthened from the existing criteria; and

b. (Must) requirements or (should) recommendations.

Change	✳ New	⊣⊢ Strengthened	– No Change

Must/ Should	⚠ Must	💡 Should

Security Vision & Responsibility - New Category

For a CTPAT Member's supply chain security to be effective, it must become an integral part of a company's culture and it must be incorporated into its core business processes. This can only be accomplished if the company's management is fully engaged in developing and maintaining the program.

ID	Criteria	Implementation Guidance	Change	Must/ Should
1	In promoting a culture of security, CTPAT Members should publicize their commitment to supply chain security and the CTPAT program through a statement of support. The statement should be signed by a senior company official and displayed throughout the company.	Statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. Senior company officials who should support and sign the statement may include the President, CEO, General Manager, or Security Director. Areas to display the statement of support include the company's website, on posters in key areas of the company (reception; packaging; warehouse; etc.), and/or be part of company security seminars, etc.	✳	💡
2	To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team. These new security measures should be included in existing company procedures, which creates a more sustainable structure and emphasizes that supply chain security is everyone's responsibility.	Supply Chain Security has a much broader scope than traditional security programs; it intertwines through many departments, along with Security, such as Human Resources, Information Technology, and import/export offices. Supply Chain Security Programs built on a more traditional, Security Department-based model may be less viable over the long run because the responsibility to carry out the security measures are concentrated with fewer employees, and, as a result, may be susceptible to the loss of key personnel.	✳	💡

ID	Criteria	Implementation Guidance	Change	Must/ Should
3	Implementing the right framework for a security program is important for its success. To ensure a program's continuity, a written multi-level review/assessment process, which includes a system of checks, balances, and accountability, must be integrated into the security framework in order to verify that the program continues to operate as designed.	A multi-level audit system involves creating an audit/review structure that corresponds to the levels of management in the company. Supervisors audit/review their direct employees, and the next level up of managers audit/review the supervisors to ensure the responsibilities assigned to each level are being fulfilled according to the design of the Supply Chain Security program. For Members with high-risk supply chains based on their risk assessments, simulation or table-top exercises may be a part of the targeted check to ensure personnel will know how to react in the event of a real security incident.	✹	⚠
4	The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the CTPAT Point(s) of Contact (POC) must provide regular updates regarding the progress or outcomes of any audits, exercises, or validations. The POCs must be knowledgeable about CTPAT's program requirements. In addition, this person must be capable of making decisions on behalf of the company in CTPAT matters.	CTPAT expects the designated POC to be a proactive individual who engages and is responsive to his or her Supply Chain Security Specialist. Members may identify additional individuals who may help support this function by listing them as contacts in the CTPAT Portal.	🏋	⚠

Change	✹ New	🏋 Strengthened	− No Change	Must/ Should	⚠ Must	💡 Should

CORPORATE SECURITY

Risk Assessment

The continued targeting of the supply chain by terrorist groups and criminal organizations underscores the need for CTPAT Members and their business partners to fully assess their existing and potential exposure to these evolving threats. Requirements in this category focus on the need for Members to conduct and update a risk assessment and the factors to consider when developing a risk assessment.

ID	Criteria	Implementation Guidance	Change	Must/ Should
5	CTPAT Members must conduct and document an overall risk assessment (RA) to identify where security vulnerabilities may exist. The RA must identify threats, quantify risks, and incorporate sustainable measures to mitigate vulnerabilities. The Member must take into account CTPAT requirements specific to the Member's role in the supply chain.	The overall risk assessment is made up of two key parts. The first part is a self-assessment of the Member's supply chain security practices, procedures, and policies within the facilities that it controls to verify its adherence to CTPAT's Minimum Security Criteria, and an overall management review of how it is managing risk. The second part of the RA is the international risk assessment. This portion of the RA includes the identification of geographical threat(s) based on the Member's business model and role in the supply chain, and a process to quantify the possible impact of each threat on the security of the Member's supply chain. CTPAT developed the Five Step Risk Assessment guide as an aid to conducting the international risk assessment portion of a Member's overall risk assessment, and it can be found on U.S. Customs and Border Protection's website at *https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf.*	🏋	⚠
6	The overall risk assessment must incorporate site-specific vulnerabilities applicable to the Member's role in the supply chain, including the extent to which the CTPAT Member relies on third parties with access to the Member's export and cargo loading operations, both inbound and outbound, as applicable.	Third parties may include seasonal dockworkers, janitorial services, contracted IT providers, etc.	🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
7	The international portion of the risk assessment must document or map the movement of the Member's cargo throughout its supply chain from the point of origin to the Importer's distribution center. The mapping must include all business partners involved both directly and indirectly in the exportation/movement of the goods. As applicable, mapping must include documenting how cargo moves in and out of transport facilities/cargo hubs and noting if the cargo is "at rest" at one of these locations for an extended period of time. Cargo is more vulnerable when "at rest," waiting to move to the next leg of its journey.	When documenting the movement of all cargo, the Member is to consider all involved parties - including those who will only be handling the documents such as customs brokers and others that may not directly handle the cargo, but may have operational control such as Non Vessel Operated Common Carriers (NVOCCs) or Third Party Logistics Providers (3PLs). If any portion of the transport is subcontracted, this may also be considered because the more layers of indirect parties, the greater risk involved.	🏋	⚠
8	Risk assessments must be reviewed annually, or more frequently as risk factors dictate.	Circumstances that may require a risk assessment to be reviewed more frequently than once a year include an increased threat level from a specific country, periods of heightened alert, following a security breach or incident, changes in business partners, and/or changes in corporate structure/ownership such as mergers and acquisitions, etc.	—	⚠
9	CTPAT Members should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption.	A crisis may include the disruption of the movement of trade data due to a cyberattack, a fire, or a Carrier driver being hijacked by armed individuals. Based on risk and where the Member operates or sources from, contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen and get back to normal operating conditions.	✳	💡

Change	✳ New	🏋 Strengthened	— No Change

Must/ Should	⚠ Must	💡 Should

CORPORATE SECURITY

Business Partners

CTPAT Members engage with a variety of business partners, both domestically and internationally. Screening business partners is a well-established criterion, but a new element has been added; Members must screen their business partners for activity related to trade based money laundering and terrorist funding.

ID	Criteria	Implementation Guidance	Change	Must/ Should
10	CTPAT Members must have a written, risk based process for screening new business partners and for monitoring current partners. Factors that must be included in this process are checks on the financial soundness of the business and activity related to money laundering and terrorist funding.	Vetting the “legitimacy” of business partners is very important. Criminals often pose as a legitimate business by creating a fake or shell company. The fake company may portray itself as an Exporter/ Importer or agent representing a company or consortium of small businesses. Or, to pretend to be a legitimate trucking company, a fake company might sign up with a freight broker to perpetrate a fictitious or fraudulent pickup. If your company uses the services of a freight broker, this is a growing industrywide threat to consider in your risk assessment. The following are some of the vetting elements that can help determine if a company is legitimate: • Verifying the company’s business address and how long they have been at that address; • Verifying land line phone numbers; • Conducting research on the internet on both the company and its principals; and • Checking business references. To help with this process, Members are encouraged to consult the document CTPAT’s Warning Indicators for Trade Based Money Laundering and Terrorism Financing Activities.	🏋	⚠

Change	✳ New	🏋 Strengthened	— No Change

Must/ Should	⚠ Must	💡 Should

ID	Criteria	Implementation Guidance	Change	Must/ Should
13	Members may choose to accept their business partners’ certification in CTPAT or an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States, as proof of meeting CTPAT’s security criteria. However, Members must obtain evidence of the certification as proof of compliance and must continue to monitor these business partners to ensure they maintain their certification.	Business partners’ CTPAT certification may be ascertained via the CTPAT Portal’s Status Verification Interface system. If the business partner certification is from a foreign AEO program under an MRA with the United States, the foreign AEO certification will include the security component. Members may visit the foreign Customs Administration’s website where the names of the AEOs of that Customs Administration are listed, or request the certification directly from their business partners. Current United States MRAs include: New Zealand, Canada, Jordan, Japan, South Korea, the European Union (28 Member States), Taiwan, Israel, Mexico, Singapore, and the Dominican Republic.	🏋	⚠

Change	✸ New	🏋 Strengthened	− No Change	Must/ Should	⚠ Must	💡 Should

ID	Criteria	Implementation Guidance	Change	Must/ Should
14	Where a CTPAT Member outsources or contracts elements of its supply chain, the Member must exercise due diligence (via visits, questionnaires, etc.) to ensure these business partners have security measures in place that meet or exceed CTPAT's MSC.	Importers tend to outsource a large portion of their supply chain activities and, as the party in the transaction that usually has leverage over its business partners, it is recommended that Importers treat security measures in the same way as they treat other contractual requirements, such as quality control measures and packaging specifications. Compliance with Importer security standards is enabled through existing mechanisms (contracts, purchase orders, etc.). When a Member has numerous supply chains, high risk areas are the priority. For those business partners that are not in CTPAT or an Authorized Economic Operator program under a Mutual Recognition Arrangement with the United States, the CTPAT Member will exercise due diligence to ensure (when it has the leverage to do so) that these business partners meet the program's security criteria that most closely pertains to the business partner's role in the supply chain. For example, if a Member has a non-CTPAT Member Highway Carrier in its supply chain, the Importer can provide this partner the criteria for Highway Carriers. If the business partner's role does not have a corresponding CTPAT entity such as a domestic/foreign warehouse, the core criteria would still pertain such as Business Partner requirements, Physical Security (based on risk), Cybersecurity, and Training. Besides providing the criteria to its business partner, the Member will ensure the business partner understands the criteria and what it can do to meet the MSC. Therefore, additional outreach and training may also be provided, if needed. Determining if a business partner is compliant with the MSC can be accomplished in several ways. Based on risk, the company may conduct an onsite audit at the facility, hire a contractor/service provider to conduct an onsite audit, or use a security questionnaire.	🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
15	If security questionnaires are used to ascertain business partners compliance with CTPAT's security requirements, questionnaire responses must be detailed, and if necessary, be supported by documentary evidence. Security questionnaires used to determine and document compliance with the program's security criteria must include the following: • Name and title of the person(s) completing it; • Date completed; • Signature of the individual(s) who completed the document; • Signature of a senior company official, security supervisor, or authorized company representative to attest to the accuracy of the questionnaire; • Provide enough detail in responses to determine compliance; and • If allowed by local security protocols, include photographic evidence, copies of policies/procedures, and copies of completed forms like instruments of international traffic (IIT) inspection checklists and/or guard logs.	Due to their role in the supply chain, some companies may receive numerous questionnaires. CTPAT does not wish to create an undue burden on these companies; therefore, Members may be flexible in obtaining the needed information. For example, an already completed questionnaire from another company may be accepted, or a business partner may provide its own document that describes how it meets the program's security criteria.	✸	⚠
16	If weaknesses are identified during business partners' security self-assessments, it must be addressed immediately and corrections must be implemented in a timely manner. Members must confirm that deficiencies have been mitigated via documentary evidence.	Documentary evidence may include copies of contracts for additional security guards, photographs taken of a newly installed security camera or intrusion alarm, etc.	✸	⚠
17	Based upon a documented risk-assessment process, CTPAT Members should require business partners to update their security self-assessments on a regular basis, or as circumstances/risks dictate.	Periodic updates to the self-assessment are important to ensure that a strong security program is still in place and operating properly. Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country, changes in source location, new critical business partners (those that actually handle the cargo, provide security to a facility, etc.).	✸	💡

CORPORATE SECURITY

Cybersecurity - New Category

Technology has evolved dramatically since CTPAT's creation in 2001. Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets - intellectual property, customer information, financial data, and employee records, among others. Companies also understand that cybersecurity can better position their organizations with business partners, customers, investors, and other stakeholders. These requirements will position CTPAT Members towards a stronger cybersecurity posture, and allow them to better deter cyberattacks and prevent loss of data.

ID	Criteria	Implementation Guidance	Change	Must/ Should
19	CTPAT Members must have comprehensive written cybersecurity policies and procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.	Members are encouraged to follow the National Institute of Standards and Technology's voluntary risk-based Framework for Improving Critical Infrastructure Cybersecurity (https://www.nist.gov/cyberframework) – a set of industry standards and best practices which help organizations manage cybersecurity risks. This Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The Framework complements, but does not replace, an organization's risk management process and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.	✷	⚠
20	To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or other unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.		✷	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
21	CTPAT Members utilizing network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.	Making sure a company network is secure is a very important task, and one that is recommended to be scheduled regularly. This can be done by conducting vulnerability scans and penetration testing. A vulnerability scan identifies open ports and IP addresses in use, as well as operating systems and software. It will then compare what it has discovered against its database of known vulnerabilities and report back. There are many free and paid versions of vulnerability scanners available. Penetration testing, on the other hand, is when existing vulnerabilities are exploited to see how much of a threat they are to the network.	✹	⚠
22	Cybersecurity policies should address how a Member shares information on cybersecurity threats with the Government and other business partners.	Members are encouraged to share information on cybersecurity threats with the Government and business partners within their supply chain. Information sharing is a key part of the Department of Homeland Security's mission to create shared situational awareness of malicious cyber activity. CTPAT Members may want to join the National Cybersecurity and Communications Integration Center (NCCIC - *https://www.us-cert.gov/nccic*). The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.	✹	💡
23	A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.		−	⚠
24	Cybersecurity policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.	An example of a circumstance that would dictate a policy update sooner than annually is a cyber attack. Using the lessons learned from the attack would help strengthen a Member's cybersecurity policy.	✹	⚠
25	User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.		🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
26	Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be safeguarded.	Complex login passwords or passphrases, biometric technologies, and electronic ID cards are three different types of authentication processes. The use of a two-factor authentication (2FA) or multi-factor authentication (MFA) process is preferred. MFAs can assist in closing network intrusions exploited by weak passwords or stolen credentials. MFA can assist in closing these attack vectors by requiring individuals to augment passwords or passphrases (something you know) with something you have, like a token, or one of your physical features - a biometric. It is recommended that if using a password, it is complex. The National Institute of Standards and Technology's (NIST) NIST Special Publication 800-63-3: Digital Identity Guidelines, includes password guidelines. It recommends the use of long, easy-to-remember passphrases instead of words with special characters. These longer passphrases are considered much harder to crack.	🏋	⚠
27	Members that allow their users to connect remotely to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to securely access the company's intranet when located outside of the office. Members must also have procedures designed to secure remote access from unauthorized users.	A VPN is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection, and access control.	✹	⚠
28	If Members allow employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.	Personal devices include storage media like CDs, DVDs, and USB flash drives. Care will be used if employees are allowed to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network.	🏋	⚠

Change	✹ New	🏋 Strengthened	− No Change

Must/ Should	⚠ Must	💡 Should

ID	Criteria	Implementation Guidance	Change	Must/ Should
29	Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.	Computer software is intellectual property (IP) owned by the entity that created it. Without the express permission of the manufacturer or publisher, it is illegal to install software, no matter how it is acquired. That permission almost always takes the form of a license from the publisher, which accompanies authorized copies of software. Unlicensed software is more likely to fail as a result of an inability to update. It is more prone to contain malware, rendering computers and their information useless. Expect no warranties or support for unlicensed software, leaving your company on its own to deal with failures. There are legal consequences for unlicensed software as well, including stiff civil penalties and criminal prosecution. Software pirates increase costs to users of legitimate, authorized software and decrease the capital available to invest in research and development of new software. Members may want to have a policy that requires Product Key Labels and Certificates of Authenticity to be kept when new media is purchased. CDs, DVDs, and USB media include holographic security features to help ensure you receive authentic products and to protect against counterfeiting.	✳	💡
30	Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format. Media used to store backups should preferably be stored at a facility offsite.	Devices used for backing up data may not be on the same network as the one used for production work.	✳	💡
31	All media, hardware, or other IT equipment must be accounted for through regular inventories. When disposed, they must be properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines.	Members may want to consult the NIST Guidelines for Media Sanitization (NIST Special Publication 800-88).	✳	⚠

TRANSPORTATION SECURITY

Conveyance and Instruments of International Traffic Security

This category covers procedures Members must have in place to prevent, detect, or deter un-manifested material and/or unauthorized personnel from gaining access to conveyances and Instruments of International Traffic (ITT). A cornerstone of the criteria in this category is security inspections of instruments of international traffic (IIT). A new component is being added to these inspections, so that any visible pest contamination is identified and mitigated.

ID	Criteria	Implementation Guidance	Change	Must/ Should
32	Conveyances and Instruments of International Traffic (IIT) must be stored (at all times) in a secure area to prevent unauthorized access and/or manipulation.		✹	⚠

Change	✹ New	⟛ Strengthened	— No Change

Must/ Should	⚠ Must	💡 Should

ID	Criteria	Implementation Guidance	Change	Must/ Should
34	Prior to loading/stuffing/packing, all conveyances and empty Instruments of International Traffic (IIT) must undergo CTPAT approved security and agricultural inspections to ensure their structures have not been modified to conceal contraband or have been contaminated with agricultural pests. A seven-point inspection on all empty containers and unit load devices (ULD), and an eight-point inspection on all empty refrigerated containers and ULDs must be conducted prior to loading/stuffing to include: 1. Front wall 2. Left side 3. Right side 4. Floor 5. Ceiling/Roof 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors 7. Outside/Undercarriage 8. Fan housing on refrigerated containers Inspections of conveyances and IIT must be systematic and must be conducted at conveyance storage yards. Where feasible, inspections must be conducted upon entering and departing the storage yards and at the point of loading/stuffing. These systematic inspections must include: Tractors: 1. Bumper/tires/rims 2. Doors, tool compartments and locking mechanisms 3. Battery box 4. Air breather 5. Fuel tanks 6. Interior cab compartments/sleeper 7. Faring/roof Trailers: 1. Fifth wheel area - check natural compartment/skid plate 2. Exterior - front/sides 3. Rear - bumper/doors 4. Front wall 5. Left side 6. Right side 7. Floor 8. Ceiling/roof 9. Inside/outside doors and locking mechanisms 10. Outside/Undercarriage	The program has uploaded training material to the Public Library Section of the CTPAT Portal on security and agricultural conveyance/ ITT inspections, including a USDA-U.S. Customs and Border Protection presentation in PDF format called "Carrier Conveyance Contamination". A new version of this presentation will be uploaded in the Fall of this year. This presentation outlines how several types of contaminants might be introduced by conveyances, the reasons for concern, U.S. Customs and Border Protection's efforts to prevent invasive species introduction, and best practices for industry to prevent conveyance contamination.	🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
35	Conveyances and IIT must be equipped with the right type of external hardware that can reasonably withstand attempts to remove it, which would allow the doors to be taken off without breaking the seal - providing access to the cargo and/or the inside of the IIT. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.		✸	⚠
36	The inspection of all conveyances and empty instruments of international traffic (IIT) must be recorded on a checklist. The following elements must be documented on the checklist: • Container/Trailer/IIT number; • Date of inspection; • Time of inspection; • Name of employee conducting the inspection; and • Specific areas of the IIT that were inspected. If the inspections are supervised, the supervisor should also sign the checklist.		🏋	⚠
37	All security inspections should be performed in an area of controlled access and, if available, monitored via cameras.		✸	💡
39	Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of International Traffic (IIT) inspections. The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border.	Supervisory searches of conveyances are conducted to counter internal conspiracies. As a best practice, supervisors can hide an item (like a toy or colored box) in the conveyance to determine if the field test screener/ conveyance operator finds it. Supervisory personnel could be a security manager, held accountable to senior management for security, or other designated management personnel.	➖	💡

ID	Criteria	Implementation Guidance	Change	Must/ Should
45	CTPAT Members should work with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.		✷	💡
47	For land border shipments that are in close proximity to the United States border, a “no-stop” policy should be implemented.	Cargo at rest is cargo at risk. Avoiding unnecessary stops for shipments that are in close proximity to the United States border is recommended.	✷	💡

Change	✷ New	🏋 Strengthened	— No Change		Must/ Should	⚠ Must	💡 Should

TRANSPORTATION SECURITY

Seal Security

The sealing of trailers and containers, to include continuous seal integrity, continues to be a crucial element of a secure supply chain. Requirements for written seal policies have been further developed, requiring Members to have a comprehensive written seal policy that addresses all aspects of seal security.

ID	Criteria	Implementation Guidance	Change	Must/ Should
61	CTPAT Members must have detailed high security seal procedures that describe how seals are issued and controlled at the facility and during transit. Written protocols must provide the steps to take if a seal is found to be altered, tampered with, or has the incorrect seal number to include documentation of the event, communication protocols to partners, and investigation of the incident. The findings from the investigation must be recorded in a report, and any corrective actions must be implemented as quickly as possible. When the Carrier or facility is a component of a larger entity, the written procedures must be maintained at the terminal/ local level. Procedures must be reviewed at least once a year. Written seal controls must include the following elements: Controlling Access to Seals • Management of seals is restricted to authorized personnel. • Secure storage. Inventory, Distribution, & Tracking (Seal Log) • Recording the receipt of new seals. • Issuance of seals recorded in log. Track seals via the log. • Only trained, authorized personnel may affix seals to IIT. Controlling Seals in Transit • Ensure that packed IITs are sealed. Seals Broken in Transit • If load examined--record replacement seal number. • The driver (or pertinent employee) must immediately notify dispatch (or applicable staff) when a seal is broken, indicate who broke it, and provide the new seal number. • The Carrier must immediately notify the shipper, broker, and Importer of the seal change and the replacement seal number. • The shipper must note the replacement seal number in the seal log. Seal Discrepancies • Hold any seal discovered to be altered or tampered with to aid in the investigation. • Investigate the discrepancy; follow-up with corrective measures (if warranted). • As applicable, report compromised seals to U.S. Customs and Border Protection and the appropriate foreign government to aid in the investigation.			⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
62	All CTPAT shipments that can be sealed must be secured immediately after loading/stuffing/packing by the responsible party and/or shipper or packer acting on the shippers behalf with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals. Qualifying cable and bolt seals are both acceptable. All seals used must be securely and properly affixed to IIT that are transporting CTPAT Members' cargo to/from the United States. If a cable seal is used, it must envelop the handle hubs of the two center vertical bars on the container/trailer doors in order to prevent the upward or downward movement of the cable. All excess cable remaining after the seal has been tightened and secured to the container/trailer must be removed. If a high security bolt seal is used, the seal must be placed on the Secure Cam position, if available, instead of the right door handle. The seal must be placed at the bottom of the center most vertical bar of the right container door. Alternatively, the bolt seal could be placed on the center most/left hand locking handle on the right container door if the secure cam position is not available. Whenever possible, it is recommended that the bolt seal be placed with the barrel portion or insert facing upward with the barrel portion above the hasp. Any packed IIT that can be sealed must be sealed. Some packed IIT cannot be sealed such as flatbed trailers, and other conveyances may vary with certain types that can be sealed and others that cannot. If a tank container has openings that can be sealed, they must be sealed, and the party filling the container is responsible for sealing it. When cargo is transported via sealable air cargo containers/IIT like Unit Load Devices (ULDs), high security seals must be used.		—	⚠
63	For commercial loads or conveyances not suitable for sealing with a high security seal, CTPAT Members must demonstrate how they ensure the integrity of their cargo while in-transit.	Describe the measures in place to ensure that bulk or open top loads, dump trailers, tractors, open van trailers, step decks, flatbeds, livestock trailers, and other types of open trailers or oversize loads (where a seal will not deter access) are secured during transit.	✸	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
66	CTPAT Members must be able to document the high security seals they use either meet or exceed the most current ISO 17712 standard.	Acceptable evidence of compliance is a copy of a laboratory testing certificate that demonstrates compliance with the ISO high security seal standard. CTPAT Members will also be aware of the tamper indicative features of the seals they purchase.	—	⚠
67	Company management or a security supervisor must conduct audits of seals that includes periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented. As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on conveyances and IIT.		✸	⚠
68	CTPAT's seal verification process must be followed to ensure all high security seals (bolt/cable) have been affixed properly to IIT, and are operating as designed. The procedure is known as the VVTT process: V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew or separate from one another.		✸	⚠

Change	✸ New	⧫ Strengthened	— No Change

Must/ Should	⚠ Must	💡 Should

TRANSPORTATION SECURITY

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain. As in other categories, this one has also been expanded to include procedures that address security audits, and the staging and loading of cargo.

ID	Criteria	Implementation Guidance	Change	Must/ Should
69	Members must have written processes for reviewing their security procedures.	All security procedures are subject to audits. It is recommended that an overall general audit be conducted periodically. Specialized areas that are key to supply chain security such as inspections and seal controls may undergo audits specific to those areas. For example, to ensure full compliance with CTPAT inspection procedures, management can conduct (and document) periodic reviews of the conveyance and IIT inspection processes.	✸	⚠
70	When cargo is staged overnight, or for an extended period of time, measures must be taken to secure the cargo from unauthorized access. Procedures to separate and secure domestic cargo from international cargo in warehouses or pre-staging areas must be in place.		✸	⚠
71	Cargo staging areas, and the immediate surrounding areas, must be inspected on a regular basis to ensure these areas remain free of visible pest contamination.	Preventative measures such as the use of baits, traps, or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas.	✸	⚠
73	The loading of cargo into containers/IIT should be supervised by a security officer/manager or other designated personnel.		✸	💡
74	As documented evidence of the properly installed seal, digital photographs should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.	Photographic evidence may include pictures taken at the point of stuffing to document evidence of the cargo markings, the loading process, the location where the seal was placed, and properly installed seal.	✸	💡

ID	Criteria	Implementation Guidance	Change	Must/ Should
75	Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time.		−	⚠
76	Cargo must be properly marked and manifested to include accurate weight and piece count. For sealed containers, Carriers may rely on the information provided in the shipper's shipping instructions.		−	⚠
77	If paper is used, forms and other import/export related documentation should be secured to prevent unauthorized use.	Measures, such as using a locked filing cabinet, can be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation.	−	💡
78	Bill of lading/manifesting procedures must ensure information in the Carrier's cargo manifest accurately reflects the information provided to the Carrier by the shipper or its agent, and is filed with U.S. Customs and Border Protection in a timely manner. Bill of lading information filed with U.S. Customs and Border Protection must show the first foreign location/facility where the Carrier takes possession of the cargo destined for the United States.		−	⚠
80	At all points of container stuffing/loading, the completed container/IIT inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.	The foreign container inspection sheet may be provided to the receiving dock prior to container arrival, so it can be used by receiving dock personnel to determine whether tampering of the seal/IIT occurred.	✸	💡

ID	Criteria	Implementation Guidance	Change	Must/ Should
81	Personnel must review the information included in import/export documents to identify or recognize suspicious cargo shipments. Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. As a resource and based on risk, CTPAT Members should take into account those CTPAT Key Warning Indicators for Money Laundering and Terrorism Financing Activities most applicable to the functions that they and/or their business entity perform in the supply chain. Highway Carrier personnel must be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments such as: • Originated from or destined to unusual locations; • Paid by cash or a certified check; • Using unusual routing methods; • Exhibit unusual shipping/receiving practices; • Provide vague, generalized, or a lack of information.		—	⚠
94	CTPAT Members must have written procedures for reporting an incident to include a description of the facility's internal escalation process. A notification protocol must be in place to report any suspicious activities or security incidents that may affect the security of the Member's supply chain. As applicable, the Member must report an incident to its SCSS, the closest Port of Entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain. Notifications should be made as soon as feasibly possible. Notification procedures must include the accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Procedures must be periodically reviewed to ensure contact information is accurate.	Examples of incidents warranting notification to U.S. Customs and Border Protection include (but are not limited to) the following: • Discovery of tampering with a container/IIT or high security seal; • An unaccounted for new seal has been applied to an IIT; • Smuggling of contraband to include people; stowaways; • Unauthorized entry into conveyances, locomotives, vessels, or aircraft carriers; • Extortion, payments for protection, threats, and/or intimidation; • Unauthorized use of a business entity identifier (i.e., Importer of Record (IOR) number, Standard Carrier Alpha (SCAC) code, etc.).	✹	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
95	Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons. Personnel must know the protocol to challenge an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.		—	⚠
96	CTPAT Members should set up a mechanism to report security related issues anonymously. When an allegation is received, it should be investigated, and if applicable, corrective actions should be taken.	Internal problems such as theft, fraud, and internal conspiracies may be reported more readily if the reporting party knows the concern may be reported anonymously. Members can set up a hotline program or similar mechanism that allows people to remain anonymous if they fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each reported item was investigated and that corrective actions were taken.	✷	💡
98	All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate.		—	⚠
99	Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.		—	💡
100	Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.		✷	💡
101	Seal numbers should be electronically printed on the bill of lading or other shipping documents.		✷	💡

Change	✷ New	🏋 Strengthened	— No Change

Must/ Should	⚠ Must	💡 Should

Agricultural Security - New Category

Agriculture is the largest industry and employment sector in the United States, an industry threatened by the introduction of foreign animal and plant contaminants such as soil, manure, seeds, and plant and animal material which may harbor invasive and destructive pests and diseases. Eliminating contaminants in all conveyances and all types of cargo may decrease cargo holds, delays and commodity returns or treatments.

ID	Criteria	Implementation Guidance	Change	Must/ Should
103	CTPAT Members must have written procedures designed to prevent pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. Pest prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).	WPM is defined as wood or wood products (excluding paper products) used in supporting, protecting, or carrying a commodity. WPM includes items such as pallets, crates, boxes, reels, and dunnage. Frequently, these items are made of raw wood that may not have undergone sufficient processing or treatment to remove or kill pests, and therefore remain a pathway for the introduction and spread of pests. Dunnage in particular has been shown to present a high risk of introduction and spread of pests. The IPPC is a multilateral treaty overseen by the United Nation's Food and Agriculture Organization that aims to secure coordinated, effective action to prevent and to control the introduction and spread of pests and contaminants. ISPM 15 includes internationally accepted measures that may be applied to WPM to reduce significantly the risk of introduction and spread of most pests that may be associated with WPM. ISPM 15 affects all wood packaging material requiring that they be debarked and then heat treated or fumigated with methyl bromide and stamped or branded with the IPPC mark of compliance. This mark of compliance is colloquially known as the "wheat stamp". Products exempt from the ISPM 15 are made from alternative materials, like paper, metal, plastic or wood panel products (i.e. oriented strand board, hardboard, and plywood).	✹	⚠

Physical Security

Requirements aligned to physical security outline the need to prevent, detect, or deter unauthorized personnel from gaining access to facilities. These are broken into procedures CTPAT Members must implement to decrease risk and technology guidelines they must follow if utilizing security technology such as intrusion alarms and video camera equipment to monitor facilities.

ID	Criteria	Implementation Guidance	Change	Must/ Should
104	All cargo handling and storage facilities, including trailer yards and offices should have physical barriers and/or deterrents that prevent unauthorized access.		🏋	💡
105	Perimeter fencing should enclose the areas around cargo handling and storage facilities. If a facility handles cargo, interior fencing should be used to secure cargo and cargo handling areas. Based on risk, additional interior fencing should segregate various types of cargo such as domestic, international, high value, and/or hazardous materials. Fencing should be regularly inspected for integrity and damage by designated personnel. If damage is found in the fencing, repairs should be made as soon as possible.	Other acceptable barriers may be used instead of fencing, such as a dividing wall or natural features that are impenetrable or otherwise impede access such as a steep cliff or dense thickets etc.	🏋	💡
107	Gates where vehicles and/or personnel enter or exit (as well as other points of egress) must be manned or monitored. Individuals and vehicles may be subject to search in accordance with local and labor laws.	It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated.	🏋	⚠
108	Private passenger vehicles must be prohibited from parking in or adjacent to cargo handling and storage areas.	In order to minimize the risk of cargo being stolen or compromised, locate parking areas outside of fence operational areas or at least at substantial distances from cargo handling and storage areas.	🏋	⚠
109	Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas.	Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.	—	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
110	Members who rely on security technologies for physical security must have written policies and procedures governing the use, maintenance, and protection of security technology. These policies must include the following: • Limit access to the locations of controls/hardware for security devices; • Procedures to test/inspect the technology on a regular basis; • Inspections include verification that equipment is correctly positioned and/or working properly; • Document the results of the inspections and performance testing; • If corrective actions are warranted, implement and document the actions taken; • Documented results must be maintained for a sufficient time for audit purposes. If third party (off-site) security monitoring resources are utilized, written agreements must be in place stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revisions(s), and systems access or denial(s). Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.	Security technology used to secure sensitive areas/access points includes alarms, access control devices, and video surveillance systems.	✹	⚠

Change	✹ New	Strengthened	− No Change	Must/ Should	⚠ Must	💡 Should

ID	Criteria	Implementation Guidance	Change	Must/ Should
111	CTPAT Members should utilize licensed/certified resources when considering the design and installation of security technology.	Today's security technology is complex and evolves rapidly. Security and fire alarm systems are often the first line of defense against theft. Often times companies purchase the wrong type of security technology that proves to be ineffective when needed and/or pay more than was necessary. Seeking qualified guidance will help a buyer select the right technology options for their needs and budget. It's important to do business with individuals who have a track record of successful integrations with this type of technology. Virtually all certifications are granted, at least in part, on some type of regulatory authority's licensing. According to the National Electrical Contractors Association (NECA), in the United States 33 states currently have licensing requirements for professionals engaged in the installation of security and alarm systems.	✹	💡
112	All security technology infrastructure must be physically secured from unauthorized access.	Security technology infrastructure includes computers, security software, electronic control panels, video surveillance or closed circuit television cameras, power and hard drive components for cameras, as well as recordings.	✹	⚠
113	Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.	A criminal trying to breach your security may attempt to disable the power to your security technology in order to circumnavigate your security technology. Thus, it is important to have an alternative source of power for your security technology. An alternative power source may be an auxiliary power generation source or backup batteries. Backup power generators may also be used for other critical systems such as lighting.	✹	💡
114	If camera systems are deployed, cameras should monitor a facility's premises and sensitive areas to deter unauthorized access. Alarms should be used to alert a company to unauthorized access into sensitive areas.	Sensitive areas for Importers and their business partners include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for IIT, areas where IIT are inspected, and seal storage areas.	✹	💡
115	If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to the import/export process.	Positioning cameras correctly is important to enable them to record as much of the physical "chain of custody," within the facilities control as possible. Specific areas of security focus would include cargo handling activities, container inspections, loading process, sealing process, conveyance arrival/exit, cargo and departure.	✹	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
116	If camera systems are deployed, cameras should have an alarm/ notification feature, which would signal a “failure to operate/record” condition.	A failure of video surveillance systems could be the result of someone disabling the system in order to breach a supply chain without leaving video evidence of the crime. The failure to operate feature can result in an electronic notification sent to predesignated person(s) notifying them that the device requires immediate attention.	✹	💡
117	If camera systems are deployed, cameras should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis.		✹	💡
118	Periodic, random reviews of the camera footage must be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed. Results of the reviews must be summarized in writing to include any corrective actions taken. The results must be maintained for a sufficient time for audit purposes.	The review of the footage is primarily geared toward the physical chain of custody to ensure the shipment remained secure. Some examples of processes that can be included in the review are cargo handling activities, container inspections, the loading process, sealing process, conveyance arrival/exit, and cargo departure, etc. **Purpose of the Review:** The purpose of the review(s) is to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses, and proscribe corrective actions in support of improvement to security processes. **Written Summary:** The summary of the review may include the date of the review, date of the footage viewed, which camera/area was the recording from, a brief description of any findings, and if warranted corrective actions. **Time to Maintain Documentation:** The time to retain the documented reviews of the footage may vary depending on the audit framework in place at the facility. A minimum of 2 to 5 years is recommended.	✹	⚠
119	Recordings of footage covering key import/export processes must be maintained for a minimum of 14 days after the shipment being monitored has arrived at the point of destination, where the container is first opened after clearing Customs.		✹	⚠

PEOPLE AND PHYSICAL SECURITY

Physical Access Controls

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

ID	Criteria	Implementation Guidance	Change	Must/ Should
120	CTPAT Members must have written procedures governing how identification badges and access devices are granted, changed, and removed. Where applicable, a personnel identification system must be in place for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties. Removal of access devices must take place upon the employee's separation from the company.	Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes, keys. Exit checklists are recommended when employees are separated from a company to ensure that all access devices have been returned and/or deactivated. For smaller companies, where personnel know each other, no identification system is required.	—	⚠
121	Visitors, vendors, and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors and service providers should be issued temporary identification. If temporary identification is used, it must be visibly displayed at all times during the visit. The registration log must include the following: • Date of the visit; • Visitor's name; • Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure.		🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
122	Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government-issued photo identification to the facility employee granting access to verify their identity. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the Highway Carrier company that employs the driver picking up the load.		—	⚠
123	A cargo pickup log must be kept to register drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it. The cargo pickup log must have the following items recorded: • Driver's name; • Date and time of arrival; • Employer; • Truck number; • Trailer number; • Time of departure; • The seal number affixed to the shipment at the time of departure.	A visitor log may double as a cargo log as long as the extra information is recorded in it.	✹	⚠
126	Prior to arrival, the Carrier must notify the facility of the estimated time of arrival for the scheduled pick up, the name of the driver, and truck number. Where operationally feasible, CTPAT Members must allow deliveries and pickups by appointment only.	Goal here is for shippers and Carriers to avoid fictitious pick ups. Fictitious pick-ups are criminal schemes that result in the theft of cargo by deception that includes truck drivers using fake IDs and /or fictitious businesses set up for the purpose of cargo theft.	✹	⚠
127	Arriving packages and mail should be periodically screened for contraband before being admitted.	Examples of such contraband include, but are not limited to, explosives, illegal drugs, and currency.	—	💡
129	Work requirements for security guards must be contained in written policies and procedures. Management must periodically verify compliance with these work instructions and policies through audits, policy reviews, and simulated exercises.	Security guards are often employed at manufacturing sites, seaports, distribution centers, Consolidators, and forwarders operating sites.	✹	⚠

PEOPLE AND PHYSICAL SECURITY

Personnel Security

A company's human resource force is a critical security asset but it can also be one of its weakest links. The MSC requirements in this section, therefore, deal with issues such as employee screening, pre-employment verifications, background checks, and the issuance of access devices.

ID	Criteria	Implementation Guidance	Change	Must/ Should
131	Application information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law.		—	⚠
132	In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors. Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position. Employee background screening should include verification of the employee's identity and criminal history that encompass City, State, Provincial, and Country databases. CTPAT Members and their business partners should factor in the results of background checks, as permitted by local statutes, in making hiring decisions. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, it may warrant more in-depth investigations.		—	💡

Change	✱ New	Strengthened	— No Change

Must/ Should	⚠ Must	💡 Should

Education, Training and Awareness

CTPAT's security criteria are designed to promote a layered security system. If one layer of security is disabled, another layer should prevent a security breach or alert a company to a breach. One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Requirements aligned to security training and threat awareness identify the specific trainings needed to ensure that employees are able to identify, prevent, and respond to security threats.

ID	Criteria	Implementation Guidance	Change	Must/ Should
135	Members must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. The training program must be comprehensive and cover all of CTPAT's security requirements. More in-depth specialized training must be given to those personnel in sensitive positions. One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to all employees and contractors on a regular basis, and newly hired employees and contractors must receive this training as part of their orientation/job skills training. Training topics should include protecting access controls, recognizing internal conspiracies, and reporting procedures for suspicious activities and security incidents. When possible, specialized training should include a hands-on demonstration. If a hands-on demonstration is conducted, the instructor should allow time for the students to demonstrate the process. Members must retain evidence of training such as training logs, sign in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.	The CTPAT program has already commenced the development of training on the new MSC. Once the MSC is finalized, the program will make the training available to its Members via the CTPAT Portal.	🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
136	Drivers and other employee(s) that conduct security and agricultural inspections of empty conveyances and instruments of international traffic (IIT) must be trained to inspect their conveyances/IIT for both security and agricultural purposes. Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures. Inspection training must include the following topics: • Signs of hidden compartments; • Concealed contraband in naturally occurring compartments; and • Signs of pest contamination.		−	⚠
138	Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the person holds. Sensitive positions include staff working directly with cargo or its documentation as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls. One training topic that must be given to employees dealing with import/export processes and documentation is corporate identity theft (and measures to prevent it).		✳	⚠
139	CTPAT Members should have measures in places to verify that the training provided met all training objectives.	Understanding the training and being able to use that training in one's position (for sensitive employees) is of paramount importance. Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that the Member may implement to determine the effectiveness of the training.	✳	💡
141	Specialized training must be provided annually to personnel who may be able to identify the warning indicators of Trade Based Money Laundering and Terrorism Financing.	Examples of personnel to receive such training include those responsible for trade compliance, security, procurement, finance, shipping, and receiving. Members may take into account the CTPAT Warning Indicators for Trade Based Money Laundering and Terrorism Financing Activities document which will be provided as a module in the CTPAT training.	🏋	⚠

ID	Criteria	Implementation Guidance	Change	Must/ Should
142	Training must be provided to applicable personnel on preventing visible pest contamination. Training must encompass pest prevention measures, regulatory requirements applicable to wood packaging materials (WPM), and identification of infested wood.	U.S. Customs and Border Protection has collaborated with the U.S. Department of Agriculture to develop training on visible pest contamination. Different training modules have been developed for the different trade environments: air, sea, and land border (Rail and Highway Carrier). These training modules will be made available to all Members via the CTPAT Portal.	✹	⚠
143	Personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.	The lack of quality training across industry sectors has been found to be one of the primary reasons companies become vulnerable to cyberattacks. Members can combat this by utilizing a robust cybersecurity training program, preferably one that is delivered to all personnel in a formal setting rather than simply through emails and slide shows.	🏋	⚠
144	Personnel operating and managing security technology systems must have received training in their operation and maintenance.	Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable for smaller enterprises.	✹	⚠
145	Training must be given on situational reporting. Employees must be trained to know what to report, how to report it, and to whom. In addition to reporting responsibilities, training must also be provided on what to do after the employee has reported the situation.	Procedures to report security incidents or suspicious activity are extremely important aspects of a security program, and training on how to report an incident can be included in the overall security training. Specialized training modules (based on job duties) may have more detailed training on reporting procedures to include specific response protocols after the incident is reported. The CTPAT training for Members will have a module around situational reporting, which will include what details of an incident needed to be reported on, by whom, when, etc.	✹	⚠

Change	✹ New	🏋 Strengthened	— No Change	Must/ Should	⚠ Must	💡 Should

CTPAT™

YOUR SUPPLY CHAIN'S STRONGEST LINK.

www.cbp.gov/ctpat

U.S. Customs and
Border Protection