AIR CARRIERS

Minimum Security Criteria Booklet

March 2020

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

U.S. Customs and Border Protection

AIR CARRIERS

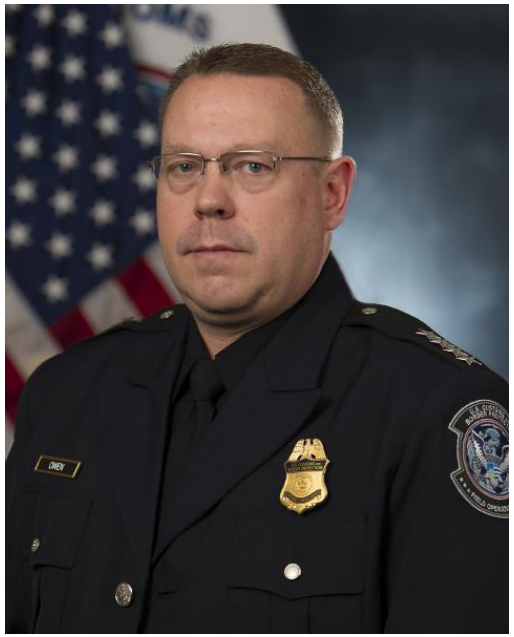
Minimum Security Criteria Booklet for Air Carriers

March 2020

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 (MSC) Booklet for Air Carriers*. Created in partnership with industry, the new MSC advances the U.S. Customs and Border Protection (CBP) mission of securing the international supply chain.

The MSC is the culmination of more than 17 years of operational experience in supply chain security, including over 30,000 CTPAT validations and revalidations. Similar documents have been created for all business entities eligible for CTPAT membership to support implementation of the new criteria and requirements.

CBP aims to approach supply chain security comprehensively. To that end, CTPAT 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 MSC maintains 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 includes 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 – Team Lead – World Business Alliance for Secure Commerce
Brandon Fried – Air Freight Forwarders/COAC
Eugene Laney – CTPAT Consolidator – DHL
Alexandra Latham – CTPAT Tier III Importer/COAC – COSTCO Wholesalers
Dan Meylor – CTPAT Broker – Carmichael
Adam Salerno – U.S. Chamber of Commerce/COAC
Michael Young – CTPAT Sea Carrier/COAC – Orient Overseas Container Line

Cybersecurity

Team B

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

Non-IT Security Technology

Team C

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

High Security Seals/Highway Carrier Issues

Team D

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

Prevention of Money Laundering and Terrorism Financing/Risk Assessment

Team E

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

Security Management and Administration

Team F

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

You are essential to the success of these requirements and serve 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 continuing our partnership.

Sincerely,

Todd C. Owen
Executive Assistant Commissioner
Office of Field Operations

TABLE OF CONTENTS

I. Introduction 9

I.1 Case for Updating and Modernizing the Criteria 9
I.2 Principles Guiding the MSC Modernization 10
I.3 Approach for Implementing the MSC 10

II. CTPAT Eligible Entity Groups and Benefits 11

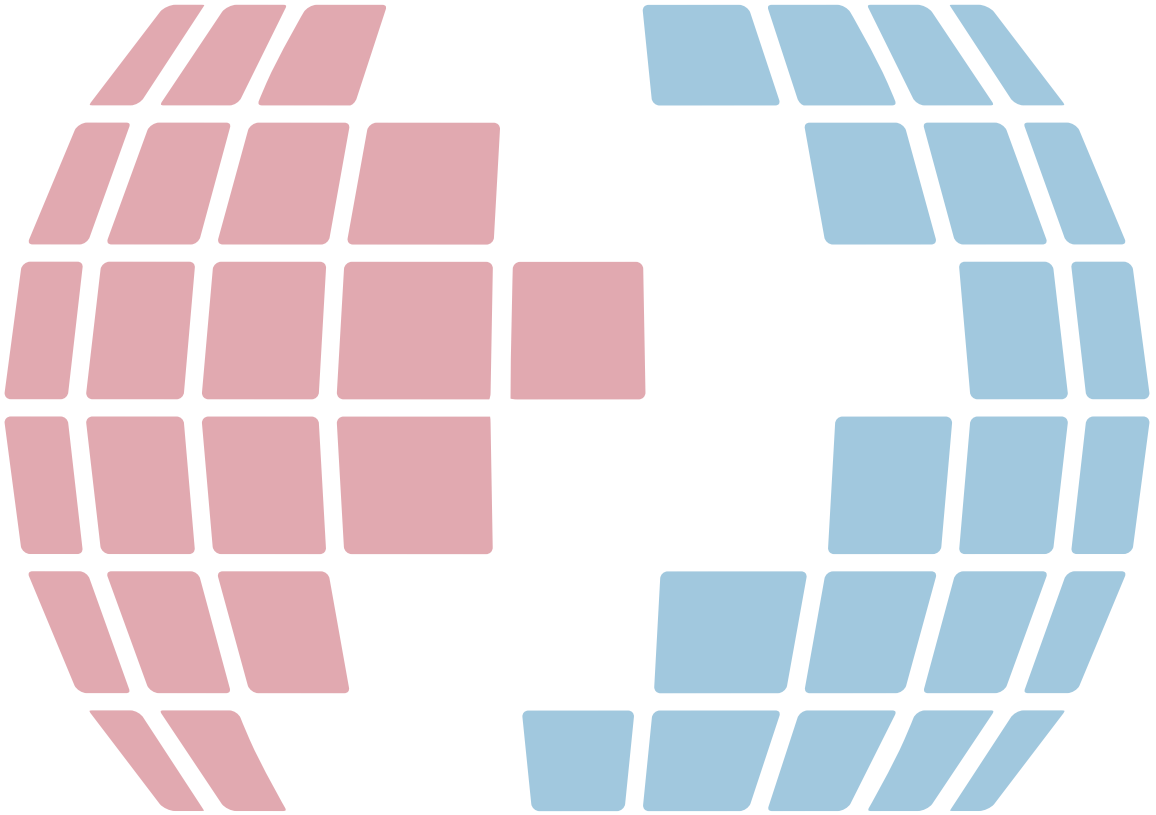
II.1 Member Benefits 11
II.2 Best Practices Framework 14

III. Minimum Security Criteria Overview and Focus Areas 16

III.1 Corporate Security 16
III.2 Transportation Security 16
III.3 People and Physical Security 17

IV. Minimum Security Criteria for Air Carriers 18

IV.1 Introduction – Key Basics 18
IV.2 Eligibility Requirements 19
IV.3 Minimum Security Criteria by Category 20



I. INTRODUCTION

The Customs Trade Partnership Against Terrorism (CTPAT) Program is a critical layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Conceived shortly after the 9/11 attacks, the Program partners with the Trade community and foreign Customs Administrations to help protect the international supply chain from terrorism, illegal contraband and other threats. CTPAT is now one of the largest and most successful public-private sector partnerships in the world designed to improve border security. Since its establishment in November 2001 with just seven major U.S. Importers, the Program today has over 11,500 Members representing the entire supply chain spectrum and accounting for over 54% of the total value of U.S. imports. As of March 2019, there were 39 Air Carriers certified in the Program.

The Minimum Security Criteria (MSC) operate as a fundamental set of building blocks to help CTPAT Members develop effective security practices that will aid them in establishing an overarching supply chain security program designed to mitigate threats to a Member's global supply chain.

I.1 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. One of these requirements mandates that the Program reviews and, if necessary, updates the MSC in consultation with the Trade. Similarly, a CTPAT Reauthorization Bill, currently in Congress, requires a biennial 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 U.S. 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% 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.

Expertise and Experience – The new MSC reflect the knowledge accumulated by CTPAT after having an operational Program in place for over 17 years. Many lessons have been learned and several vulnerabilities to the supply chain have been identified after having conducted thousands of validations around the world, and dozens of post-incident analysis or PIAs. These PIAs take place following a security breach to determine where the supply chain was compromised. The MSC also reflect the knowledge and expertise of the trade community itself.

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. The update to the MSC aims to close gaps in the supply chain given today's threat environment. Cyberattacks, for instance, have increased dramatically in the past few years, affecting all types and sizes of businesses.

I.2 Principles Guiding the MSC Modernization

Four key principles guided the process to update the MSC:

Partnership with the Trade – From the beginning of the process, CBP worked hand-in-hand with the COAC's Global Supply Chain Subcommittee, CTPAT Members, and other key Trade partners in updating the MSC.

Bidirectional Education – The Trade's perspectives and recommendations were given full consideration and the MSC reflect the input and knowledge of both the Trade and CBP.

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.

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

I.3 Approach for Implementing the MSC

Based on guidance from the Trade, CTPAT *recommends* Members implement the MSC under a phased approach throughout 2019. The following phased implementation timeline was determined via an assessment of security impact (how much more secure the supply chain will be by implementing the criteria in this category) and level of effort (how difficult it will be to implement the criteria):

Phase 1 – Cybersecurity; Conveyance and Instruments of International Traffic (IIT) Security; Seal Security

Phase 2 – Education, Training, and Awareness; Business Partner Security; Risk Assessment

Phase 3 – Security Vision and Responsibility; Physical Security; Physical Access Controls

Phase 4 – Agricultural Security; Personnel Security; Procedural Security

CTPAT validations based on the new MSC will begin in early 2020. CTPAT Members should work closely with their Supply Chain Security Specialists (SCSS) to ensure their security profile is up to date in the CTPAT Portal and the criteria in this document have been implemented.

II. CTPAT ELIGIBLE ENTITY GROUPS AND BENEFITS

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

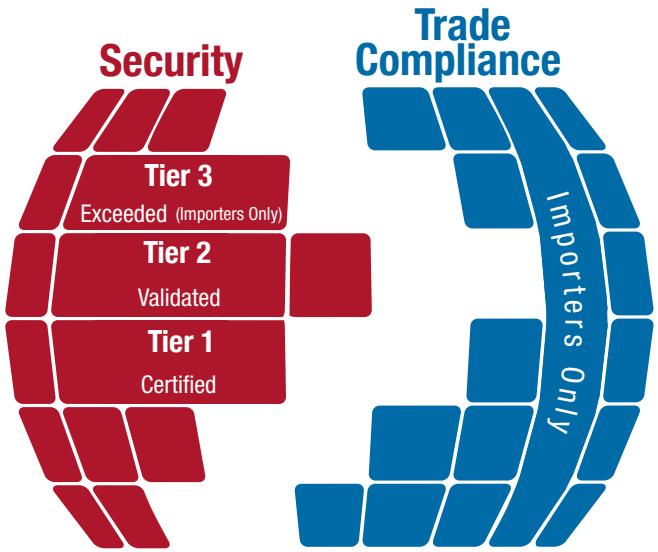
U.S. Exporters	U.S. Importers	Foreign Manufacturers (Canada and Mexico)	Mexican Long Haul Highway Carriers
Air Carriers	Rail Carriers	Sea Carriers	U.S. Highway Carriers (Canada and Mexico)
Third Party Logistics Providers (3PLs)	Consolidators	U.S. Marine Port Authority & Terminal Operators	U.S. Customs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

II.1 Member Benefits

CTPAT encompasses both supply chain security and trade compliance. The following benefits apply to the respective Memberships. At this point, only U.S. Importers that meet the security requirements of the Program are eligible for CTPAT Trade Compliance. CTPAT hopes to expand trade compliance eligibility in the near future to other entities in the supply chain.

CTPAT

YOUR SUPPLY CHAIN'S STRONGEST LINK.



Rail Carriers • Exporters • Importers • Sea Carriers
Air Carriers • Mexican Long Haul Highway Carriers
Marine Port Authority & Terminal Operators • Brokers
Highway Carriers • 3PLs • Consolidators
Foreign Manufacturers

CTPAT SECURITY BENEFITS

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:

- **Assignment of a Supply Chain Security Specialist (SCSS):** The SCSS serves as an advisor to the company and helps the CTPAT Member improve and maintain its security posture.
- **Advanced Qualified Unlading Approval ("AQUA Lane"):** Expedited clearance of sea vessels through the AQUA Lane, creating an average cost savings of $3,250 per hour per vessel for low risk sea carriers.
- **Free and Secure Trade (FAST) Lanes:** Shorter wait times at land border ports of entry via the FAST Lanes.
- **Front of the Line:** When feasible for ports, CTPAT shipments are moved ahead of any non-CTPAT shipments if selected for an exam. 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, terrorist attack, or port closure.
- **Mutual Recognition Arrangements (MRAs):** Expedited screening with worldwide security partners from a number of 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 Annual 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 team of SCSSs, who assess 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.

CTPAT TRADE COMPLIANCE BENEFITS

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. As part of this effort, CTPAT is working with its 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 under a single Program.

- **National Account Manager (NAM):** Access to an assigned National Account Manager (NAM), who acts as an advisor and liaison between CBP Headquarters and the CTPAT Trade Compliance Member.
- **Multiple Business Units:** Opportunity to apply for coverage of multiple business units.
- **Removal from Focused Assessments Pool:** Members are 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.
- **Importer Trade Activity (ITRAC) Data Access and Automation:** U.S. Importer Members will be able to access their ITRAC data directly from the CTPAT Trade Compliance Portal, and Members will be provided with the tools to evaluate that data.
- **CTPAT Trade Compliance Portal:** *(In Development)* Access to the Trade Compliance section of the CTPAT Portal to access and update information related to Trade Compliance.
- **Expedited Rulings:** Rulings and Internal Requests that are being adjudicated by the National Commodities Division will have priority and be placed at the front of the queue for processing within 20 days by the receiving office. Rulings that are not bound by the National Commodities Division's 20-day limit are also eligible for expedited rulings.
- **Release of Goods to Premises for Exam:** *(In Development)* Importers who file an entry in an Automated Commercial Environment (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 Non-Intrusive Inspections:** *(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)* The process to request manifest confidentiality for cargo manifest data as described in 19 CFR 103.31 will be automated through the CTPAT Portal.

CTPAT SECURITY AND TRADE COMPLIANCE BENEFITS

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

- **Penalty Mitigation:** CBP's Fines, Penalties and Forfeitures Division will ensure that the company's Trusted Trader status is taken into consideration and that any penalties will be offset by the measure/level of the corrective actions taken to prevent a future occurrence.
- **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:** *(Pilot is operational)* In an effort to combat Importer identity theft and provide a new benefit to CTPAT Importers, CBP is in the process of developing a multilevel approach to protect CTPAT participants from exploitation of identity theft by creating a notification and verification system.

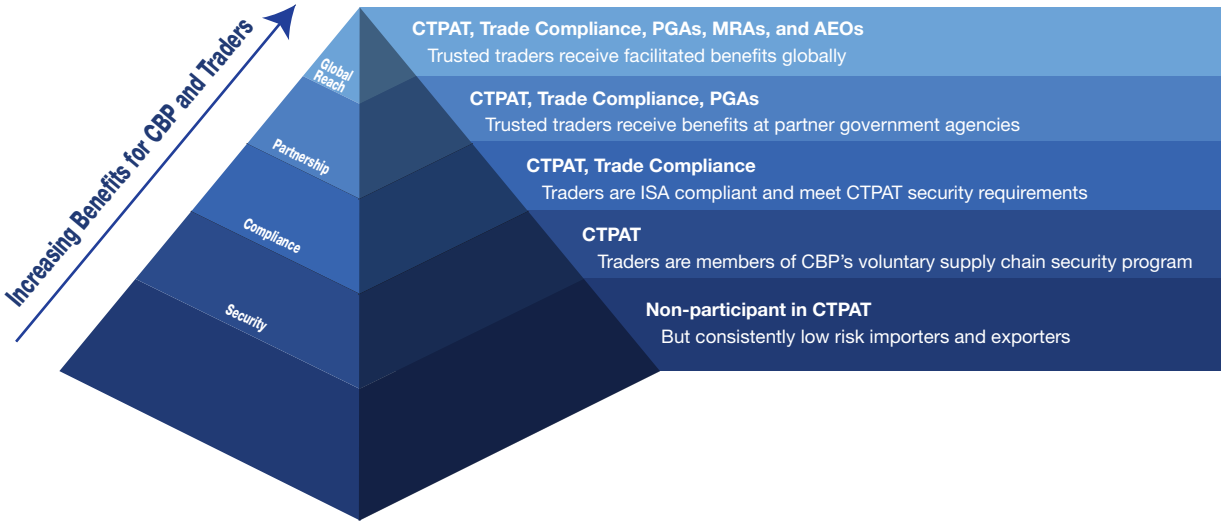


Figure 1: CTPAT – Security and Trade Compliance: Working with Partner Government Agencies (PGAs) and Authorized Economic Operator (AEO) Programs from Foreign Customs Administrations through Mutual Recognition Arrangements (MRAs).

II.2 Best Practices Framework

CTPAT Importer Members must exceed the MSC to achieve Tier III status. Previously, Members exceeded the MSC by complying with specific lists of best practices that CBP published. This led to CTPAT Members using the catalogue to pick up best practices without demonstrating that they were in fact meeting any particular set of standards – a framework.

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:

1. Senior management support;
2. Innovative technology, process or procedures;
3. Documented process;
4. Verifiable evidence; and
5. A regular system of checks, balances and accountability.

The best practices framework was tested and validated in 2018 by Members of the MSC Working Group.

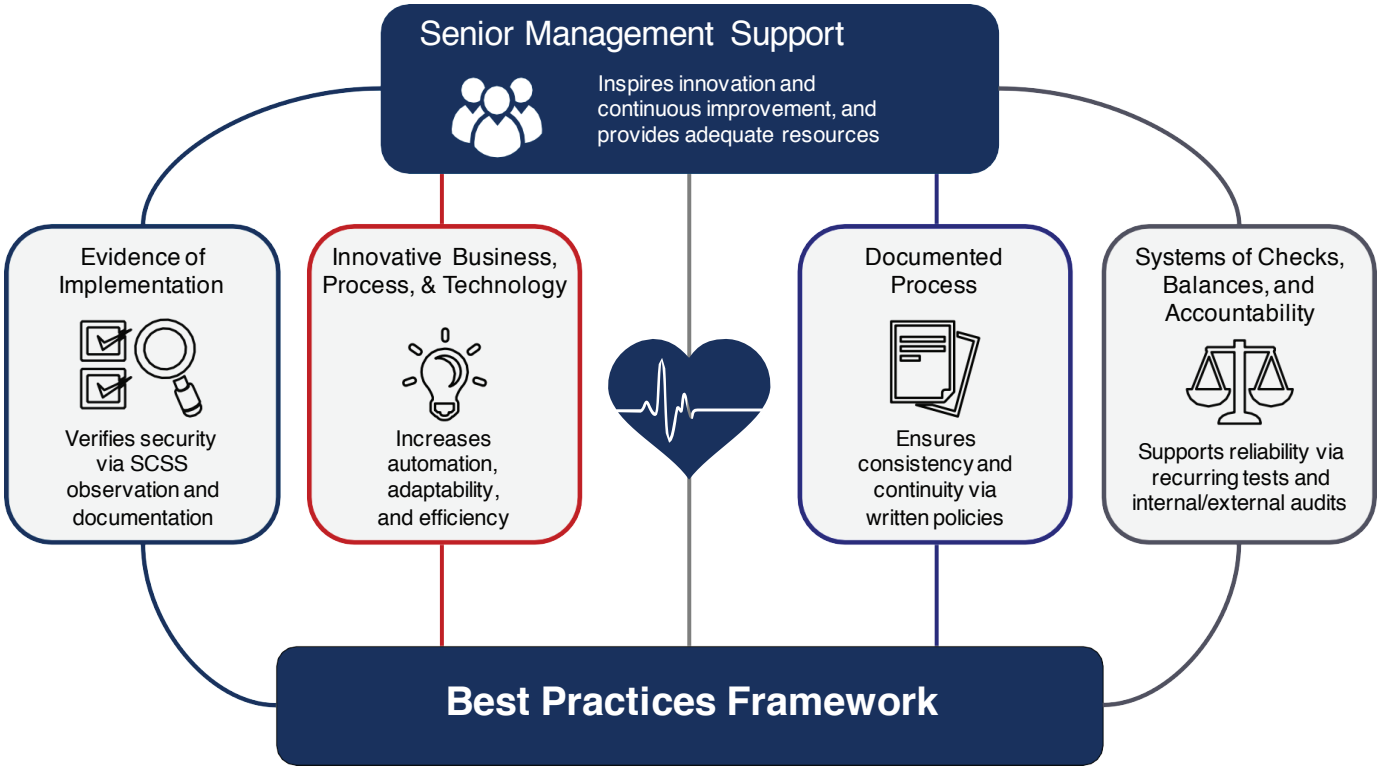


Figure 2: Best Practices Framework

III. MINIMUM SECURITY CRITERIA OVERVIEW/ FOCUS AREAS

The new criteria take a more comprehensive approach towards supply chain security; they include new requirements and recommendations in the following areas:

- Cybersecurity – To help ensure the security of critical IT systems and the trade data that moves across cyberspace;
- Agricultural Security – To protect the supply chain from agricultural contaminants and pests;
- Prevention of trade based money laundering and terrorist financing; and
- Using security technology, including security cameras and intrusion alarms, to fortify existing physical security requirements.

Other requirements in well-known categories have been strengthened. For example, under the Physical Access Control category, CTPAT added the requirement that if security guards are used, work instructions for these guards must be outlined in written procedures. Also, in an effort to highlight an issue of serious concern to CBP and which has had an impact on the supply chain, CTPAT added a recommendation that addresses a social compliance program.

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

III.1 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 companywide culture of security, implementing a system of checks and balances, expanding cybersecurity protocols, and training personnel on supply chain security best practices.

III.2 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 such as containers, trailers, and Unit Load Devices (ULDs);
- Complying with security seal protocols; and
- Maintaining operational security of cargo in transit.

The new criteria category in this focus area, Agricultural Security, aims to prevent the international supply chain from agricultural pests and contaminants.

III.3 People and Physical Security:

The people and physical security focus area encompass well known criteria for securing facilities and training personnel. The education of employees is a key component of the criteria, and as such, training of personnel on the importance of security is now a Program 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.

Focus Areas	Criteria Categories
Corporate Security	1. Security Vision and Responsibility (New)
	2. Risk Assessment
	3. Business Partner Security
	4. Cybersecurity (New)
Transportation Security	5. Conveyance and Instruments of International Traffic Security
	6. Seal Security
	7. Procedural Security
	8. Agricultural Security (New)
People and Physical Security	9. Physical Access Controls
	10. Physical Security
	11. Personnel Security
	12. Education, Training, and Awareness

IV. MINIMUM SECURITY CRITERIA FOR AIR CARRIERS

IV.1 Introduction – Key Basics

CTPAT recognizes the complexity of international supply chains, and the diverse business models Members employ. For CTPAT purposes, a business model refers to key characteristics about the business that are considered when determining if the company meets the criteria, such as the role of the company in the supply chain, size of the business, type of legal entity, number of supply chains, and number of business partners.

CTPAT encourages the implementation of security measures based upon risk analysis, and the Program allows for flexibility and the customization of security plans based on the Member's business model and the level of risk as ascertained from the Member's own risk assessment.

Some actors in the supply chain are able to better influence their business partners' security practices. Importers are the driving force in the importation process and have the leverage to require that their business partners comply with CTPAT's MSC. Regardless of how much leverage a Member has in regard to influencing business partners' practices, CTPAT expects its Members to exercise due diligence in pursuit of obtaining business partners' compliance with the Program's criteria.

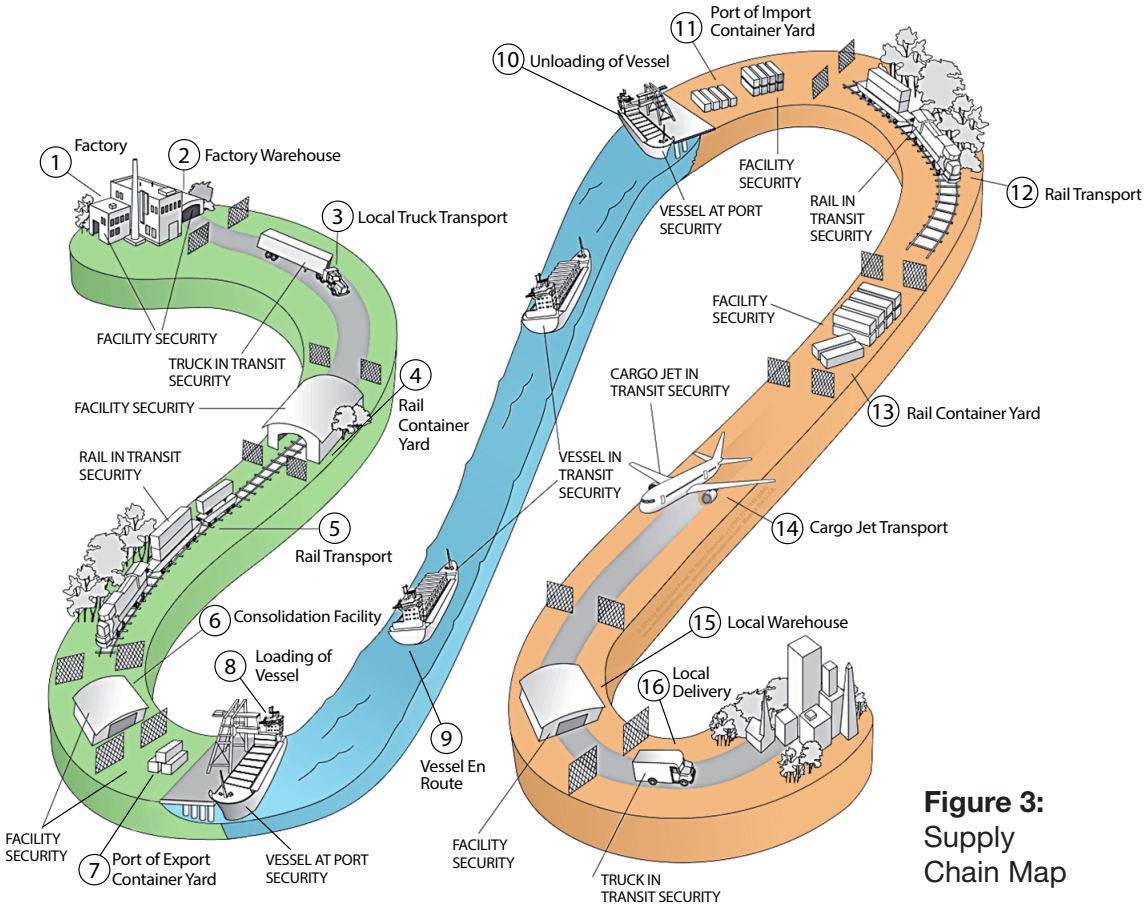


Figure 3: Supply Chain Map

CTPAT is aware of the fact that Air Carriers are already subject to defined security mandates such as the *Aviation and Transportation Security Act* (PL 107-71) of 2001. It is not the intention of the program to duplicate existing security requirements. Instead, CTPAT seeks to build upon established foundations and require additional security measures and practices which enhance the overall security of the supply chain. The program also aims to integrate Federal efforts to find smarter and more cost-effective ways to maximize resources and expertise from across the U.S. Government. To this end, CBP signed a Memorandum of Understanding with the Transportation Security Administration in 2015.

CTPAT Air Carriers must cooperate fully with CBP and other U.S. Department of Homeland Security law enforcement agencies, and upon request, provide information related to the arrival of cargo/aircraft/passengers from foreign countries, to the extent permitted by law.

Because flexibility is a cornerstone of the Program, many of the criteria do not contain specific time frames. Vague language such as "periodic" or "regular basis" is used to allow Members to customize their security programs to fit their circumstances.

For those criteria that require written procedures, it is understood that these procedures are being followed or have been implemented by the CTPAT Member – as applicable.

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

IV.2 Eligibility Requirements

As a voluntary supply chain security program based on trust, CTPAT is open to members of the trade community who can demonstrate excellence in supply chain security practices and who have had no significant security related events. While each application to the CTPAT program is considered on an individual basis, applicants need to take into account that if issues of concern do exist, they may result in CBP determining the applicant to be ineligible for participation in the program.

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

- Be an active Air Carrier that transports (within the last year) cargo shipments to the U.S.
- Have an active International Air Transport Association (IATA) Code.
- Possess a valid continuous international carrier bond registered with CBP.
- Designate a company officer that will be the primary cargo security officer responsible for CTPAT.
- Sign the "CTPAT-Partner Agreement to Voluntarily Participate" and demonstrate commitment to the obligations outlined in this Agreement. This document is signed by a Company officer when the company applies for CTPAT membership via the CTPAT Portal.
- Complete a supply chain security profile in the CTPAT Portal, identifying how the company meets and maintains the Program's MSC for Air Carriers.
- 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.

IV.3 Minimum Security Criteria By Category

Must/ Should	Must	Should

CORPORATE SECURITY

1. Security Vision & Responsibility

For a CTPAT Member's supply chain security program to become and remain effective, it must have the support of a company's upper management. Instilling security as an integral part of a company's culture and ensuring that it is a companywide priority is in large part the responsibility of the company's leadership.

ID	Criteria	Implementation Guidance	Must/ Should
1.1	In promoting a culture of security, CTPAT Members should demonstrate 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 in appropriate company locations.	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.	
1.2	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 is intertwined with Security, in many departments 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 among fewer employees, and, as a result, may be susceptible to the loss of key personnel.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
1.3	The supply chain security program must be designed with, supported by, and implemented by an appropriate written review component. The purpose of this review component is to document that a system is in place whereby personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed. The review plan must be updated as needed based on pertinent changes in an organization's operations and level of risk.	The goal of a review for CTPAT purposes is to ensure that its employees are following the company's security procedures. The review process does not have to be complex. The Member decides the scope of reviews and how in-depth they will be - based on its role in the supply chain, business model, level of risk, and variations between specific locations/sites. Smaller companies may create a very simple review methodology; whereas, a large multi-national conglomerate may need a more extensive process, and may need to consider various factors such as local legal requirements, etc. Some large companies may already have a staff of auditors that could be leveraged to help with security reviews. A Member may choose to use smaller targeted reviews directed at specific procedures. Specialized areas that are key to supply chain security such as inspections and seal controls may undergo reviews specific to those areas. However, it is useful to conduct an overall general review periodically to ensure that all areas of the security program are working as designed. If a member is already conducting reviews as part of its annual review, that process could suffice to meet this criterion. For members with high-risk supply chains (determined by their risk assessment), simulation or tabletop exercises may be included in the review program to ensure personnel will know how to react in the event of a real security incident.	
1.4	The company's point(s) of contact (POC) to CTPAT must be knowledgeable about CTPAT program requirements. These individuals need to provide regular updates to upper management on issues related to the program, including the progress or outcomes of any audits, security related exercises, and CTPAT validations.	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.	

2. Risk Assessment

Must/ Should	Must	Should

The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for Members to assess existing and potential exposure to these evolving threats. CTPAT recognizes that when a company has multiple supply chains with numerous business partners, it faces greater complexity in securing those supply chains. When a company has numerous supply chains, it should focus on geographical areas/supply chains that have higher risk.

When determining risk within their supply chains, Members must consider various factors such as the business model, geographic location of suppliers, and other aspects that may be unique to a specific supply chain.

Key Definition:

Risk – A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. What determines the level of risk is how likely it is that a threat will happen. A high probability of an occurrence will usually equate to a high level of risk. Risk may not be eliminated, but it can be mitigated by managing it – lowering the vulnerability or the overall impact on the business.

ID	Criteria	Implementation Guidance	Must/ Should
2.1	CTPAT Members must conduct and document the amount of risk in their supply chains. CTPAT Members must conduct an overall risk assessment (RA) to identify where security vulnerabilities may exist. The RA must identify threats, assess 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 (RA) 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. When looking at the possible impact of each threat on the security of the member's supply chain, the member needs a method to assess or differentiate between levels of risk. A simple method is assigning the level of risk between low, medium, and high. 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* For Members with extensive supply chains, the primary focus is expected to be on areas of higher risk.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
2.3	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.	
2.4	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 return to normal operating conditions.	

3. Business Partners

Must/ Should	Must	Should

CTPAT Members engage with a variety of business partners, both domestically and internationally. For those business partners who directly handle cargo and/or import/export documentation, it is crucial for the Member to ensure that these business partners have appropriate security measures in place to secure the goods throughout the international supply chain.

When business partners subcontract certain functions, an additional layer of complexity is added to the equation, which must be considered when conducting a risk analysis of a supply chain.

Key Definition:

Business Partner – A business partner is any individual or company whose actions may affect the chain of custody security of goods being imported to or exported from the United States via a CTPAT Member's supply chain. A business partner may be any party that provides a service to fulfill a need within a company's international supply chain. These roles include all parties (both directly and indirectly) involved in the purchase, document preparation, facilitation, handling, storage, and/or movement of cargo for, or on behalf, of a CTPAT Importer or Exporter Member. Two examples of indirect partners are subcontracted carriers and overseas consolidation warehouses – arranged for by an agent/logistics provider.

ID	Criteria	Implementation Guidance	Must/ Should
3.1	CTPAT Members must have a written, risk based process for screening new business partners and for monitoring current partners. A factor that Members should include in this process is checks on activity related to money laundering and terrorist funding. To assist with this process, please consult CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities.	The following are examples of 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; • Conducting research on the internet on both the company and its principals; • Checking business references; and • Requesting a credit report. Examples of business partners that need to be screened are direct business partners such as manufacturers, product suppliers, pertinent vendors/service providers, and transportation/logistics providers. Any vendors/service providers that are directly related to the company's supply chain and/or handle sensitive information/equipment are also included on the list to be screened; this includes brokers or contracted IT providers. How in-depth to make the screening depends on the level of risk in the supply chain.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
3.4	The business partner screening process must take into account whether a partner is a CTPAT Member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA). Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners, and Members must obtain evidence of the certification and 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, the Dominican Republic, and Peru.	

ID	Criteria	Implementation Guidance	Must/ Should
3.5	When 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 Minimum Security Criteria (MSC).	Importers and exporters tend to outsource a large portion of their supply chain activities. Importers (and some exporters) are the parties in these transactions that usually have leverage over their business partners and can require that security measures are implemented throughout their supply chains, as warranted. For those business partners that are not CTPAT or accepted MRA members, 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 applicable security criteria. To verify adherence to security requirements, importers conduct security assessments of their business partners. The process to determine how much information is to be gathered regarding a business partner's security program is based on the member's risk assessment, and if there are numerous supply chains, high-risk areas are the priority. 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. If security questionnaires are used, the level of risk will determine the amount of detail or evidence required to be collected. More details may be required from companies located in high-risk areas. If a Member is sending a security questionnaire to its business partners, consider requiring the following items: •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 •Based on risk, and if allowed by local security protocols, include photographic evidence, copies of policies/procedures, and copies of completed forms like Instruments of international traffic inspection checklists and/or guard logs. *Signatures may be electronic. If a signature is difficult to obtain/ verify, the respondent may attest to the questionnaire's validity via email, and that the responses and any supporting evidence was approved by a supervisor/manager (name and title are required).	

ID	Criteria	Implementation Guidance	Must/ Should
3.7	To ensure their business partners continue to comply with CTPAT's security criteria, Members should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate.	Periodically reviewing business partners' security assessments is important to ensure that a strong security program is still in place and operating properly. If a member never required updates to its assessment of a business partner's security program, the Member would not know that a once viable program was no longer effective, thus putting the member's supply chain at risk. Deciding on how often to review a partner's security assessment is based on the Member's risk assessment process. Higher risk supply chains would be expected to have more frequent reviews than low risk ones. If a Member is evaluating its business partner's security by in person visits, it may want to consider leveraging other types of required visits. For example, cross-train personnel that test for quality control to also conduct security verifications. 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.).	

4. Cybersecurity

Must/ Should	Must	Should

In today's digital world, cybersecurity is the key to safeguarding a company's most precious assets – intellectual property, customer information, financial and trade data, and employee records, among others. With increased connectivity to the internet comes the risk of a breach of a company's information systems. This threat pertains to businesses of all types and sizes. Measures to secure a company's information technology (IT) and data are of paramount importance, and the listed criteria provide a foundation for an overall cybersecurity program for Members.

Key Definitions:

Cybersecurity – Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change or destruction. It is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken.

Information Technology (IT) – IT includes computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.

ID	Criteria	Implementation Guidance	Must/ Should
4.1	CTPAT Members must have comprehensive written cybersecurity policies and/or 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 cybersecurity protocols that are based on recognized industry frameworks/standards. The *National Institute of Standards and Technology (NIST) is one such organization that provides a Cybersecurity Framework (https://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines, and practices to help manage and reduce cybersecurity risks 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 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. *NIST is a non-regulatory federal agency under the Department of Commerce that promotes and maintains measurement standards, and it is the technology standards developer for the federal government.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
4.2	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 another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.		
4.3	CTPAT Members using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.	A secure computer network is of paramount importance to a business, and ensuring that it is protected requires testing on a regular basis. This can be done by scheduling vulnerability scans. Just like a security guard checks for open doors and windows at a business, a vulnerability scan (VS) identifies openings on your computers (open ports and IP addresses), their operating systems, and software through which a hacker could gain access to the company's IT system. The VS does this by comparing the results of its scan against a database of known vulnerabilities and produces a correction report for the business to act upon. There are many free and commercial versions of vulnerability scanners available. The frequency of the testing will depend on various factors including the company's business model and level of risk. For example, companies should run these tests whenever there are changes to a business's network infrastructure. However, cyber-attacks are increasing among all sizes of businesses, and this needs to be considered when designing a testing plan.	
4.4	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.	

ID	Criteria	Implementation Guidance	Must/ Should
4.5	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.		
4.6	Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.	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.	
4.7	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.		
4.8	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. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.	To guard IT systems against infiltration, user access must be safeguarded by going through an authentication process. Complex login passwords or passphrases, biometric technologies, and electronic ID cards are three different types of authentication processes. Processes that use more than one measure are preferred. These are referred to as two-factor authentication (2FA) or multi-factor authentication (MFA). MFA is the most secure because it requires a user to present two or more pieces of evidence (credentials) to authenticate the person's identity during the log-on process. MFAs can assist in closing network intrusions exploited by weak passwords or stolen credentials. MFAs 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. If using passwords, they need to be complex. The National Institute of Standards and Technology's (NIST) NIST Special Publication 800-63B: Digital Identity Guidelines, includes password guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html). It recommends the use of long, easy to remember passphrases instead of words with special characters. These longer passphrases (NIST recommends allowing up to 64 characters in length) are considered much harder to crack because they are made up of an easily memorized sentence or phrase.	
4.9	Members that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.	VPNs are not the only choice to protect remote access to a network. Multi-factor authentication (MFA) is another method. An example of a multi-factor authentication would be a token with a dynamic security code that the employee must type in to access the network.	

ID	Criteria	Implementation Guidance	Must/ Should
4.10	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 must be taken 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.	
4.11	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.	
4.12	Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.	Data backups should take place as data loss may affect individuals within an organization differently. Daily backups are also recommended in case production or shared servers are compromised/ lose data. Individual systems may require less frequent backups, depending on what type of information is involved. Media used to store backups should preferably be stored at a facility offsite. Devices used for backing up data should not be on the same network as the one used for production work. Backing up data to a cloud is acceptable as an "offsite" facility.	
4.13	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.	Some types of computer media are hard drives, removable drives, CD-ROM or CD-R discs, DVDs, or USB drives. The National Institute of Standards and Technology (NIST) has developed the government's data media destruction standards. Members may want to consult NIST standards for sanitization and destruction of IT equipment and media. Media Sanitization: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	

TRANSPORTATION SECURITY

5. Conveyance and Instruments of International Traffic Security

Must/ Should	Must	Should

Smuggling schemes often involve the modification of conveyances and Instruments of International Traffic (IIT), or the hiding of contraband inside IIT. This criteria category covers security measures designed to prevent, detect, and/or deter the altering of IIT structures or surreptitious entry into them, which could allow the introduction of unauthorized material or persons.

At the point of stuffing/loading, procedures need to be in place to inspect IIT and properly seal them. Cargo in transit or "at rest" is under less control, and is therefore more vulnerable to infiltration, which is why seal controls and methods to track cargo/conveyances in transit are key security criteria.

Breaches in supply chains occur most often during the transportation process; therefore, Members must be vigilant that these key cargo criteria be upheld throughout their supply chains.

Key Definition:

Instruments of International Traffic (IIT)– IIT includes containers, flatbeds, unit load devices (ULDs), lift vans, cargo vans, shipping tanks, bins, skids, pallets, caul boards, cores for textile fabrics, or other specialized containers arriving (loaded or empty), in use or to be used in the shipment of merchandise in international trade.

ID	Criteria	Implementation Guidance	Must/ Should
5.1	Conveyances and Instruments of International Traffic (IIT) must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instruments of International Traffic or (as applicable) allow the seal/doors to be compromised.	The secure storage of conveyances and IIT (both empty and full) is important to guard against unauthorized access.	
5.2	The CTPAT inspection process must have written procedures for both security and agricultural inspections.	With the prevalence of smuggling schemes that involve the modification of conveyances or Instruments of International Traffic, it is imperative that Members conduct inspections of conveyances and Instruments of International Traffic to look for visible pests and serious structural deficiencies. Likewise, the prevention of pest contamination via conveyances and IIT is of paramount concern, so an agricultural component has been added to the security inspection process. Pest contamination is defined as visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).	

ID	Criteria	Implementation Guidance	Must/ Should
5.3	CTPAT Members must ensure that the following systematic CTPAT security and agricultural inspections are conducted. Requirements for these inspections will vary depending upon if the supply chain is land-based (Canada or Mexico) or if the supply chain originates overseas (ocean and air modes). Prior to stuffing/packing, all empty Instruments of International Traffic (IIT) must be inspected, and conveyances must also be inspected when they are crossing land borders into the United States. <u>Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight:</u> A seven-point inspection must be conducted on all empty containers and unit load devices (ULDs); and an eight-point inspection must be conducted on all empty refrigerated containers and ULDs: 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; and 8. Fan housing on refrigerated containers. <u>Additional inspection requirements for land border crossings via highway carriers:</u> Inspections of conveyances and IIT must be conducted at conveyance/IIT 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 17-point inspections: **<u>Tractors:</u>** 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; and 7. Faring/roof. **<u>Trailers:</u>** 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; and 10.Outside/Undercarriage.	Security and agricultural inspections are conducted on instruments of international traffic (IIT) and conveyances to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests. Expectations for overseas supply chains are to inspect all IIT at the point of stuffing/packing. However, if an ocean/air based supply chain is higher risk, it may warrant including more extensive inspection procedures to include conveyances and/or inspections at marine port terminals or air logistics facilities. Usually, there are higher levels of risk involved in shipments with land border crossings, which is why both the conveyance and IIT undergo multiple inspections. Some examples of IIT for various modes are ocean containers, refrigerated containers/trailers, over-the-road trailers, flatbed trailers, tank containers, rail/boxcars, hoppers, and unit load devices (ULDs). The Public Library Section of the CTPAT Portal contains training material on security and agricultural conveyance/Instruments of International Traffic inspections.	

ID	Criteria	Implementation Guidance	Must/ Should
5.5	The inspection of all conveyances and empty Instruments of International Traffic should be recorded on a checklist. The following elements should be documented on the checklist: • Container/Trailer/Instruments of International Traffic number; • Date of inspection; • Time of inspection; • Name of employee conducting the inspection; and • Specific areas of the Instruments of International Traffic that were inspected. If the inspections are supervised, the supervisor should also sign the checklist. The completed container/Instruments of International Traffic inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.		
5.6	All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.		

ID	Criteria	Implementation Guidance	Must/ Should
5.10	Before departure, aircraft must undergo thorough inspections to ensure they are free of pest contamination and for security purposes. Upon arrival, aircraft inspections must verify the proper disposal of unfinished meals and other organic waste (regulated garbage) via companies approved for the effective disposal of these items. The following areas must be inspected for security reasons • All baggage/cargo *hold areas; • All *galleys, *stores, and food carts; • All overheads; • All lavatories; • Cockpit and areas housing electronic equipment; • Exterior inspection of all wheel wells and landing gears; • Avionic compartments and bays as warranted. *Must also be inspected for pest contamination	Both of these inspections (security and pest contamination) may be conducted simultaneously. Per Title 7 the Code of Federal Regulations (CFR) 330.400 -330.403 and Title 9 CFR 94.5, regulated garbage arriving on means of conveyances from foreign regions, other than Canada, is allowed entry under certain conditions. Garbage arriving from Hawaii, the U.S. territories and/or U.S. possessions is also allowed entry under certain conditions. The United States Department of Agriculture (USDA) defines “trash” as refuse that neither contains nor is visually contaminated with regulated garbage. For example, trash that solely contains empty soda cans would be unrestricted. Newspapers and magazines in the passenger cabin would also be unrestricted. An empty cardboard milk carton, sandwich, or fruit found in the passenger cabin, however, would be considered as regulated garbage as opposed to trash and would be restricted. Garbage, per USDA, is all waste material that is derived in whole or in part from fruits, vegetables, meats, or other plant or animal (including poultry) material, and other refuse of any character whatsoever that has been associated with any such material. Garbage is regulated by USDA’s Animal and Plant Health Inspection Service (APHIS) when the garbage is on or removed from a means of conveyance, if the means of conveyance has been in any port outside the United States and Canada within the previous two-year period or to any port in Hawaii or any United States territory. Refer to “APHIS/Plant Protection Quarantine (PPQ) Compliance Agreement” (PPQ Form 519). Most airline carriers have already contracted companies that have demonstrated compliance with APHIS regulated garbage regulations.	
5.13	When an Air Carrier allows a Unit Load Device (ULD) to leave their control, written procedures must be in place to track the ULD and its return into the carrier’s custody. Security procedures must include transport from the cargo area to the aircraft.		
5.29	If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the Member must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate.		

6. Seal Security

Must/ Should	Must	Should

The sealing of trailers and containers to attain continuous seal integrity, continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security, such as using the correct seals per CTPAT requirements; properly placing a seal on IIT, and verifying that the seal has been affixed properly.

ID	Criteria	Implementation Guidance	Must/ Should
6.1	CTPAT Members must have detailed, written high-security seal procedures that describe how seals are issued and controlled at the facility and during transit. Procedures must provide the steps to take if a seal is altered, tampered with, or has the incorrect seal number, including documentation of the event, communication protocols to partners, and investigation of the incident. The findings from the investigation must be documented, and any corrective actions must be implemented as quickly as possible. These written procedures must be maintained at the local operating level so that they are easily accessible. Procedures must be reviewed at least once a year and updated as necessary. 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 Instruments of International Traffic (IIT). **Controlling Seals in Transit:** • When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering. • Confirm the seal number matches what is noted on the shipping documents. **Seals Broken in Transit:** • If a load is examined, record the replacement seal number. • The driver must immediately notify dispatch when a seal is broken, indicate who broke the seal, 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:** • Retain altered or tampered seals to aid in investigations. • Investigate the discrepancy; follow-up with corrective measures (if warranted). • As applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation.		

ID	Criteria	Implementation Guidance	Must/ Should
6.2	All CTPAT shipments that can be sealed must be secured immediately after loading/stuffing/packing by the responsible party (i.e. the shipper or packer acting on the shipper's behalf) with a high-security seal that meets or exceeds the most current International Organization for Standardization (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 Instruments of International Traffic that are transporting CTPAT Members' cargo to/from the United States.	The high-security seal used 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 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. If a bolt seal is being used, it is recommended that the bolt seal be placed with the barrel portion or insert facing upward with the barrel portion above the hasp.	
6.4	In instances where cargo is not transported in a Unit Load Device (ULD), security methods must be put in place to ensure, to the greatest extent possible, cargo is rendered tamper resistant and/or tamper evident.	Any packed IIT that can be sealed must be sealed. Some packed Instruments of International Traffic 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.	
6.5	CTPAT Members (that maintain seal inventories) must be able to document that the high-security seals they use 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 are expected to be aware of the tamper indicative features of the seals they purchase.	
6.6	If a Member maintains an inventory of seals, company management or a security supervisor must conduct a seal audit 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 Instruments of International Traffic.		

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
6.7	CTPAT's seal verification process must be followed to ensure all high-security seals (bolt/cable) have been affixed properly to Instruments of International Traffic, 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, separate from one another, or any part of the seal becomes loose.	When applying cable seals, they need to envelop the rectangular hardware base of the vertical bars in order to eliminate any upward or downward movement of the seal. Once the seal is applied, make sure that all slack has been removed from both sides of the cable. The VVTT process for cable seals needs to ensure the cables are taut. Once it has been properly applied, tug and pull the cable in order to determine if there is any cable slippage within the locking body.	

7. Procedural Security

Must/ Should	Must	Should

Procedural Security encompasses many aspects of the import-export process, documentation, and cargo storage and handling requirements. Other vital procedural criteria pertain to reporting incidents and notification to pertinent law enforcement. Additionally, CTPAT often requires that procedures be written because it helps maintain a uniform process over time. Nevertheless, the amount of detail needed for these written procedures will depend upon various elements such as a company's business model or what is covered by the procedure.

CTPAT recognizes that the technology used in supply chains continues to evolve. The terminology used throughout the criteria references written, paper-based procedures, documents, and forms. Electronic documents and signatures, and other digital technologies, however, are also acceptable ways to document required procedures.

The CTPAT Program is not designed to be a "one size fits all" model. Each company must decide (based on its risk assessment) how to implement and maintain procedures. However, it is more effective to incorporate security processes within existing procedures rather than create a separate manual for security protocols. This creates a more sustainable structure and helps emphasize that supply chain security is everyone's responsibility.

ID	Criteria	Implementation Guidance	Must/ Should
7.3	Passenger flights carrying cargo must have developed (risk based) written policies and procedures for passenger aircraft transporting cargo to include more intrusive examination of the cargo prior to packaging and loading, such as x-ray inspections.		Must
7.7	If paper documents are 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.	Should
7.8	The shipper or its agent must ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, and carriers must exercise due diligence to ensure these documents are accurate. BOLs and manifests must be filed with U.S. Customs and Border Protection (CBP) in a timely manner. BOL information filed with CBP must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States. The weight and piece count must be accurate.	When picking up sealed Instruments of International Traffic, carriers may rely on the information provided in the shipper's shipping instructions. Requiring the seal number to be electronically printed on the bill of lading (BOL) or other export documents helps guard against changing the seal and altering the pertinent document(s) to match the new seal number. However, for certain supply chains, goods may be examined in transit, by a foreign Customs authority, or by CBP. Once the seal is broken by the government, there needs to be a process to record the new seal number applied to the IIT after examination. In some cases, this may be handwritten.	Must

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
7.23	CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process. A notification protocol must be in place to report any suspicious activities or security incidents (such as drug seizures, discovery of stowaways, etc.) that take place anywhere around the world and which affects the security of the member's supply chain. As applicable, the Member must report any global incidents to its Supply Chain Security Specialist (SCSS), the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain. Notifications to CBP must be made as soon as feasibly possible and in advance of any conveyance or IIT crossing the border. 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; • Discovery of a hidden compartment in a conveyance or IIT; • An unaccounted new seal has been applied to an IIT; • Smuggling of contraband, including 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.).	
7.24	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.		
7.25	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.	
7.29	Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.		
7.32	Carriers must comply with CBP's Advance Passenger Information System (APIS) requirements. Procedures must be in place to record and report all anomalies regarding passenger and/or crew to CBP or other law enforcement agencies.		

ID	Criteria	Implementation Guidance	Must/ Should
7.37	Following a significant security incident, Members must initiate a post-incident analysis immediately after becoming aware of the incident and in order to determine where the supply chain may have been compromised. This analysis must not impede/interfere with any known investigations conducted by a government law enforcement agency. The company's post-incident analysis findings must be documented, completed as soon as feasibly possible, and, if allowed by law enforcement authorities, made available to the SCSS upon request.	A security incident is a breach in which security measures have been circumvented, eluded, or violated, and have resulted or will result in a criminal act. Security incidents include acts of terrorism, smuggling (narcotics, human, etc.), and the presence of stowaways.	

8. Agricultural Security

Must/ Should	Must	Should

Agriculture is the largest industry and employment sector in the U.S., 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 CBP cargo holds, delays and commodity returns or treatments. Ensuring compliance with CTPAT's agricultural requirements will also help protect a key industry in the U.S. and the overall global food supply.

Key Definition:

Pest contamination – The International Maritime Organization defines pest contamination as visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).

ID	Criteria	Implementation Guidance	Must/ Should
8.1	CTPAT Members must, in accordance with their business model, have written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. Visible 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).	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

9. Physical Security

Must/ Should	Must	Should

Cargo handling and storage facilities, Instruments of International Traffic storage areas, and facilities where import/export documentation is prepared in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.

One of the cornerstones of CTPAT is flexibility, and security programs should be customized to fit each company's circumstances. The need for physical security can vary greatly based on the Member's role in the supply chain, its business model, and level of risk.

The physical security criteria provides a number of deterrents/obstacles that will help prevent unwarranted access to cargo, sensitive equipment, and/or information, and Members should employ these security measures throughout their supply chains.

ID	Criteria	Implementation Guidance	Must/ Should
9.1	All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.		
9.2	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.	
9.4	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.	
9.5	Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.	Locate parking areas outside of fenced and/or operational areas - or at least at substantial distances from cargo handling and storage areas.	
9.6	Adequate lighting must be provided inside and outside the facility including, as appropriate, 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.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
9.7	Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas.	Electronic security technology used to secure/monitor sensitive areas and access points includes: burglary alarm systems (perimeter and interior) –these are also known as Intrusion Detection Systems (IDS); access control devices; and video surveillance systems (VSS) -including Closed Circuit Television Cameras (CCTVs). A CCTV/ VSS system could include components such as Analog Cameras (coax-based), Internet Protocol-based (IP) cameras (network-based), recording devices, and video management software. Secure/sensitive areas, which would benefit from video surveillance, may include: cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yard and storage areas for Instruments of International Traffic (IIT), areas where IIT are inspected, and seal storage areas.	
9.8	Members who rely on security technology for physical security must have written policies and procedures governing the use, maintenance, and protection of this technology. At a minimum, these policies and procedures must stipulate: • That access to the locations where the technology is controlled or managed is limited to authorized personnel; • The procedures that have been implemented to test/inspect the technology on a regular basis; • That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly; • That the results of the inspections and performance testing is documented; • That if corrective actions are necessary, they are to be implemented as soon as possible and the corrective actions are documented; • That the documented results of these inspections be maintained for a sufficient time for audit purposes. If a third party central monitoring station (off-site) is used, the CTPAT Member must have written procedures stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revisions, and systems access or denials. Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.	Security technology needs to be tested on a regular basis to ensure it is working properly. There are general guidelines to follow: • Test security systems after any service work and during and after major repairs, modifications, or additions to a building or facility. A system's component may have been compromised, either intentionally or unintentionally. • Test security systems after any major changes to phone or internet services. Anything that might affect the system's ability to communicate with the monitoring center should be double-checked. • Make sure video settings such as motion activated recording; motion detection alerts; images per second (IPS), and quality level, have been set up properly. • Make sure camera lenses (or domes that protect the cameras) are clean and lenses are focused. Visibility should not be limited by obstacles or bright lights. • Test to make sure security cameras are positioned correctly and remain in the proper position (cameras may have been deliberately or accidentally moved).	

ID	Criteria	Implementation Guidance	Must/ Should
9.9	CTPAT Members should use licensed/certified resources when considering the design and installation of security technology.	Today's security technology is complex and evolves rapidly. Oftentimes companies purchase the wrong 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. According to the National Electrical Contractors Association (NECA), in the U.S. 33 states currently have licensing requirements for professionals engaged in the installation of security and alarm systems.	
9.10	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.	
9.11	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 it. 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.	
9.12	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, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for Instruments of International Traffic (IIT), areas where IIT are inspected, and seal storage areas.	
9.13	If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to the import/export process. Cameras should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis.	Positioning cameras correctly is important to enable the cameras to record as much as possible of the physical "chain of custody" within the facility's control. Based on risk, key areas or processes may include cargo handling and storage; shipping/receiving; the cargo loading process; the sealing process; conveyance arrival/exit; IT servers; container inspections (security and agricultural); seal storage; and any other areas that pertain to securing international shipments.	

ID	Criteria	Implementation Guidance	Must/ Should
9.14	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.	
9.15	If camera systems are deployed, 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 in accordance with the law. 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.	If camera footage is only reviewed for cause (as part of an investigation following a security breach etc.), the full benefit of having cameras is not being realized. Cameras are not only investigative tools. If used proactively, they may help prevent a security breach from occurring in the first place. Focus the random review of the footage on the physical chain of custody to ensure the shipment remained secure and all security protocols were followed. Some examples of processes that may be reviewed are the following: • Cargo handling activities; • Container inspections; • The loading process; • Sealing process; • Conveyance arrival/exit; and • Cargo departure, etc. **Purpose of the review:** The review is intended to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses, and prescribe corrective actions in support of improvement to security processes. Based on risk (previous incidents or an anonymous report on an employee failing to follow security protocols at the loading dock, etc.), the Member may target a review periodically. **Items to include in the written summary:** • The date of the review; • Date of the footage that was reviewed; • Which camera/area was the recording from; • Brief description of any findings; and • If warranted, corrective actions. If a breach were to happen, an investigation would need to be conducted, and maintaining any camera footage that covered the packing (for export) and loading/sealing processes would be of paramount importance in discovering where the supply chain may have been compromised. For monitoring, the CTPAT program recommends allotting at least 14 days after a shipment has arrived at its first point of distribution. This is where the container is first opened after clearing Customs.	

ID	Criteria	Implementation Guidance	Must/ Should
9.16	If cameras are being used, recordings of footage covering key import/ export processes should be maintained on monitored shipments for a sufficient time to allow an investigation to be completed.	If a breach were to happen, an investigation would need to be conducted, and maintaining any camera footage that covered the packing (for export) and loading/sealing processes would be of paramount importance in discovering where the supply chain may have been compromised. For monitoring, the CTPAT program recommends allotting at least 14 days after a shipment has arrived at its first point of distribution. This is where the container is first opened after clearing Customs.	

10. Physical Access Controls

Must/ Should	Must	Should

Access controls prevent unauthorized access into facilities/areas, help maintain control of employees and visitors, and protect company assets. Access controls include the positive identification of all employees, visitors, service providers, and vendors at all points of entry.

ID	Criteria	Implementation Guidance	Must/ Should
10.1	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 when the employees separate from the company.	Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes, and keys. When employees are separated from a company, the use of exit checklists help ensure that all access devices have been returned and/or deactivated. For smaller companies, where personnel know each other, no identification system is required. Generally, for a company with more than 50 employees, an identification system is required.	
10.2	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 should be escorted. In addition, 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.		

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
10.8	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.	
10.9	Delivery of goods to the consignee or other persons accepting delivery of cargo at the partner's facility should be limited to a specific monitored area.		
10.10	If security guards are used, work instructions for security guards must be contained in written policies and procedures. Management must periodically verify compliance and appropriateness with these procedures through audits and policy reviews.	Though guards may be employed at any facility, they are often employed at manufacturing sites, seaports, distribution centers, storage yards for Instruments of International Traffic, consolidator, and forwarders operating sites.	

PEOPLE AND PHYSICAL SECURITY

11. Personnel Security

Must/ Should	Must	Should

A company's human resource force is one of its most critical assets, but it may also be one of its weakest security links. The criteria in this category focus on issues such as employee screening and pre-employment verifications.

Many security breaches are caused by internal conspiracies, which is where one or more employees collude to circumvent security procedures aimed at allowing an infiltration of the supply chain. Therefore, Members must exercise due diligence to verify that employees filling sensitive positions are reliable and trustworthy. 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.

ID	Criteria	Implementation Guidance	Must/ Should
11.1	Written processes must be in place to screen prospective employees and to periodically check current employees. Application information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law.	CTPAT is aware that labor and privacy laws in certain countries may not allow all of the application information to be verified. However, due diligence is expected to verify application information when permitted.	
11.2	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, encompassing 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.		
11.5	CTPAT Members must have an Employee Code of Conduct that includes expectations and defines acceptable behaviors. Penalties and disciplinary procedures must be included in the Code of Conduct. Employees/contractors must acknowledge that they have read and understood the Code of Conduct by signing it, and this acknowledgement must be kept in the employee's file for documentation.	A Code of Conduct helps protect your business and informs employees of expectations. Its purpose is to develop and maintain a standard of conduct that is acceptable to the company. It helps companies develop a professional image and establish a strong ethical culture. Even a small company needs to have a Code of Conduct; however, it does not need to be elaborate in design or contain complex information.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

12. Education, Training and Awareness

Must/ Should	Must	Should

CTPAT's security criteria are designed to form the basis of a layered security system. If one layer of security is overcome, another layer should prevent a security breach, or alert a company to a breach. Implementing and maintaining a layered security program needs the active participation and support of several departments and various personnel.

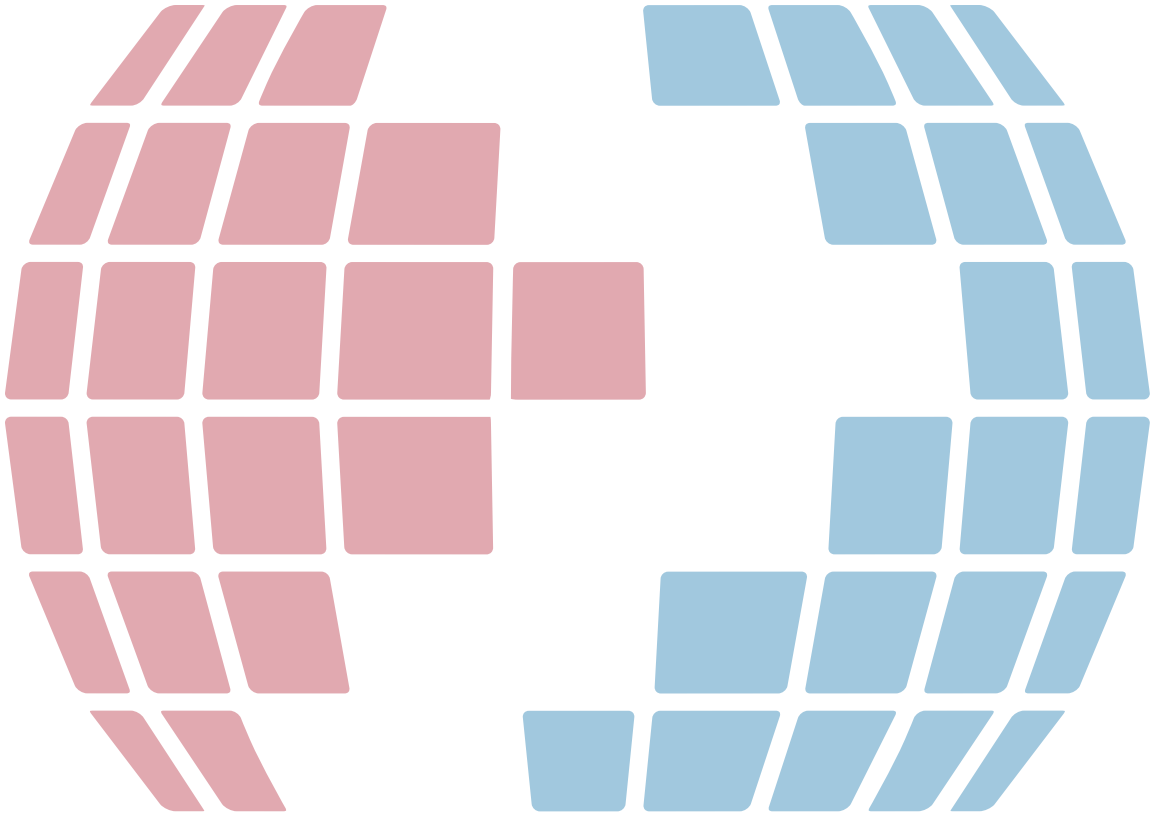
One of the key aspects to maintaining a security program is training. Educating employees on what the threats are and how their role is important in protecting the company's supply chain is a significant aspect to the success and endurance of a supply chain security program. Moreover, when employees understand why security procedures are in place, they are much more likely to adhere to them.

ID	Criteria	Implementation Guidance	Must/ Should
12.1	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. Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds. 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 employees, as required, based on their functions and position on a regular basis, and newly hired employees must receive this training as part of their orientation/job skills training. 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.	Training topics may 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. For CTPAT purposes, sensitive positions include staff working directly with import/export 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.	

Note: Criteria ID numbers not listed are not applicable to Air Carriers.

ID	Criteria	Implementation Guidance	Must/ Should
12.2	Drivers and other personnel 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.		
12.4	CTPAT Members should have measures in place 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.	
12.7	Training must, in accordance with the Member's business model, 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.	
12.8	As applicable, based on their functions and/or positions, 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.	Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.	

ID	Criteria	Implementation Guidance	Must/ Should
12.9	Personnel operating and managing security technology systems must receive operations and maintenance training in their specific areas. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable.		
12.10	Personnel must be trained on how to report security incidents and suspicious activities.	Procedures to report security incidents or suspicious activity are extremely important aspects of a security program. 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, including specifics on the process, such as, what to report, to whom, how to report the incident, and what to do after the report is completed.	



CTPAT™

YOUR SUPPLY CHAIN'S STRONGEST LINK.

CTPAT PROGRAM

CBP.GOV/CTPAT

1300 Pennsylvania Avenue, NW
Washington, DC 20229
OFO-INDUSTRYPARTNERSHIP@cbp.dhs.gov

U.S. Customs and Border Protection

CBP Publication # 1102-0520