CTPAT Course for Customs Broker Personnel

Source: GISTnet

One of the critical aspects of maintaining and sustaining the CTPAT security program is training. The education of employees is a vital component of the "people and physical security" focus area of the minimum security criteria (MSC). Training of personnel to recognize threats, foster awareness of vulnerabilities, and understand the important role each person plays in securing the supply chain is a requirement of the CTPAT program.

This basic-level course is designed to meet the CTPAT requirements for all employees who must understand, perform or otherwise comply with operational security measures. It will encompass all of the minimum security focus areas and the categories that "must" be met. We begin with the requirements for all CTPAT members and their business partners. The course continues by discussing the benefits, eligibility requirements, and specific criteria for customs brokers and ends with those specified for importers. The information regarding importers is included because MSC 12.5 requires that customs brokers must be able to explain CTPAT's security requirements to their importer clients, apprise them of critical program developments, and encourage them to become CTPAT members.

Important: This course also applies to supervisors and managers that do not have additional responsibilities for administering the CTPAT program for their company. Supervisors and managers that have the responsibility of setting-up, documenting, administering, and ensuring compliance with their company's CTPAT program should take *S12u--CTPAT for Customs Broker Mangers, Supervisors and CTPAT Administrators*. S12u contains more in-depth coverage including information on the application and proper completion of the security profile, certification, and validation requirements.

According to MSC 12.1, 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. This course is suitable for both initial and refresher training.

CTPAT Introduction

CTPAT is an ongoing compliance effort consisting of mandatory security requirements that must be met based on certain types of businesses in the supply chain. Why do companies want to participate in CTPAT? In this lesson we begin to look at the specific requirements for participation and benefits based on business type.

General—Threats that Go beyond Purely Commercial Concern

In addition to routine *commercial* cargo and supply chain vulnerabilities (*i.e.,* theft and damage) which are addressed under shipper, carrier or warehouse "loss prevention" programs, there are governmental concerns over cargo supply chain security. These include:

- Collecting Customs duty and tax – Smuggling and other forms of commercial import fraud have been major government concerns since customs duty, toll levies and other taxes first became a source of government revenue.
- Blocking illicit drugs and other contraband – This is another traditional government concern and includes the detection of these items inserted into legitimate shipments as a means of smuggling.
- Protecting public health and safety – Preventing the commerce in and smuggling of items that could adversely affect public health and safety and the health of animals and agriculture is a government responsibility for which safety regulations are imposed on a wide range of products. The transportation of "dangerous goods" is highly regulated and measures are taken to detect and prevent inadvertent transportation of pests and disease.
- Implementing national security and policy – In pursuit of national security and public policy objectives, governments also regulate the shipment of arms and military equipment, strategic technology, potentially detrimental items of interest to adversaries, and scarce resources.

These concerns bring the involvement of governments and international organizations into the realm of cargo and supply chain security.

In addition to national and regional governments, the World Customs Organization (WCO), International Maritime Organization, and International Civil Aviation Organization (ICAO) are concerned with eliminating or reducing supply chain threats and mitigating the public safety and commercial effects of accidental and hostile acts involving cargo transportation and commerce.

To address threats including smuggling, piracy, hijacking, and terrorist threats, supply chain treats and vulnerabilities are subject to government regulation, preventive measures, incident response, and mitigation programs.

Smuggling

Smuggling is and has been a problem wherever governments collect customs duty and tax on goods being shipped in or out of a country, or otherwise exercise controls over what can be legally imported or exported.

Examples of goods that are frequently smuggled include:

- Illicit drugs, other contraband products
- cash
- Arms and military equipment imported or exported without required permits
- Counterfeit goods
- Goods subject to import restrictions like quotas or import licenses
- Goods subject to high tax and duty rates

Legitimate importers, exporters and transportation carriers will occasionally have their cargo, intermodal containers and conveyances used for smuggling without their knowledge. Here the security challenge is to prevent the *insertion* of excess items into the cargo, and the subsequent removal of the same. Most of the time, this type of smuggling involves someone on the *inside*, like an employee or a legitimate facility visitor such as a truck driver.

Today, in addition to traditional smuggling, terrorist use of legitimate supply chains to smuggle weapons and supplies has become a huge concern. Legitimate organizations want to prevent terrorists from infiltrating their supply chains!

Piracy and Vessel Hijacking

Concern over piracy and hijacking of vessels at sea goes back to antiquity and today remains a serious problem in parts of the world such as the South China Sea or off the coast of Somalia.

These events cause loss of life, loss of cargo, and general supply chain disruption. National governments have responded with law enforcement and military efforts, including intelligence gathering through informants, patrolling high risk waters, various vessel protective counter-measures, and the search, capture and prosecution of pirates.

The U.N. and IMO have responded to piracy with conventions and international standards aimed at preventing air piracy, and most nations have adopted these conventions into law. See International Convention for the Safety of Life at Sea (SOLAS).

Air Piracy, Aircraft Hijacking

Beginning in the late 1950s aircraft hijacking has also become a problem. Most air hijackings have had motives of theft, ransom, political blackmail, or transportation to a particular destination. The U.N. and ICAO responded with conventions and international standards aimed at preventing air piracy, and most nations have adopted these conventions and measures into law.

Terrorist Threats

Due to more frequent and serious incidents, terrorism, of both international and domestic origin, has become the single most important national security concern of many governments.

Global trade and supply chains, and all modes of cargo transportation, have been significantly impacted by government efforts to combat terrorism. For more on this topic, refer to heading Global Terrorism—Today's Major New Threat.

Changing Methods and Targets as Governments Tighten Security

As security in symbolic targets and aircraft improves we can also expect terrorists to change their tactics and employ new methods, new modes of transportation, and means of attack such as biohazards and radioactive materials. Even small quantities of these substances can cause major contamination, death and community disruption. Bio-agents are the most insidious of all.

For this reason, today's *transportation* security measures must encompass *all* transportation modes and *all* threats, for example:

- Hijacking and piracy of conveyances – Increased and more effective passenger screening; protection of ships at sea, on inland waterways and in harbors; prevention of unauthorized access to aircraft while on the ground; and, better security of trucks, routing that provides less opportunity for hijacking and theft, more secure rest/fuel facilities, on-board tracking systems that detect

and notify dispatchers of any variance from planned routes, driver emergency alarms, etc.

- Destructive attacks against conveyances – An important goal is to prevent the destruction and harm of conveyances and passengers while underway, and the detonation of dangerous goods while being transported, especially near densely populated areas and critical transportation infrastructure elements. Security measures focus on keeping unauthorized people and boats away from ships, aircraft, trucks and rail lines, including all facilities. This is done by patrolled/monitored security zones around seaports and airports to prevent missile attacks, and missile counter-measures on-board aircraft. Trucks, especially those carrying dangerous goods, are routed to provide less opportunity for attack. Rail lines, stations and facilities are more aggressively monitored for suspicious people, vehicles and packages.
  International dangerous goods regulations now contain requirements for transportation security plans and the training of personnel in security techniques, with national dangerous goods regulations further strengthening these requirements.
- Theft of dangerous goods and weapons while in transit – Cargo theft has and will always be a problem which shippers and transportation carriers endeavor to prevent. Security and safety become a more compelling requirement for cargo of particular interest to terrorists. Traditional methods such as control of information ("need-to-know" access to documents, automated records, and voice communication), neutral marks and numbers, and especially personnel security and background checks are the key measures. In addition to physical security of facilities and conveyances, especially non-moving conveyances.
- Unauthorized insertion of undeclared items into shipments and transportation conveyances – This has always been a concern with respect to commercial smuggling, transportation of illegal aliens, and undeclared ("hidden") dangerous goods. Now we add terrorist weapons and terrorists themselves to this concern. To help prevent smuggling of all types, but with a new sense of urgency based on the terrorist threat, national customs authorities have increased their operational security measures and created programs to involve importers, carriers and other supply chain service providers in additional supply chain security measures. The World Customs Organization (WCO) has also been developing the "WCO Framework of Standards to Secure and Facilitate Global Trade" to harmonize security measures throughout the world. These measures include high security seals for inbound and in-bond trucks and intermodal containers, and the screening of cargo prior to shipment at the origin port based on advanced manifest

information and the ability of the destination country to have suspicious cargo inspected before loading on board the inbound conveyance.

From Government Reaction to Pro-action

In response to 9-11, and to combat the continuing long term terrorist threat, U.S. government agencies continue to implement a wide range of measures to *prevent* terrorist acts within the U.S. and against U.S. interests worldwide.

The U.S. government effort is to prevent weapons and terrorist supplies from being:

1. Acquired or produced in the U.S. – These include a variety of measures that have been taken by the Department of Homeland Security (DHS) and other specialized agencies, such as BATF, APHIS and the CDC, to control access to and commerce in explosives, toxins, biohazards, and the like.
2. Transported into, within or from the U.S. – These include CBP programs such as the Importer Security Filing (ISF), the Container Security Initiative (CSI), and Customs Trade Partnership Against Terrorism (CTPAT), plus Advance Electronic Cargo Information (AECI) of inbound and outbound shipments via all transport modes. Under the Bioterrorism Act of 2002, the U.S. FDA requires registration of all facilities (domestic and foreign) involved in the processing, packaging, transportation and storage of food which is distributed in the U.S., and advanced notice/screening of food shipments FDA Prior Notice before importation into the U.S. Finally, the U.S. DOT has mandated that shippers, transportation carriers and transportation intermediaries shipping, carrying or arranging certain types and quantities of dangerous goods transportation have a Hazardous Materials Security Plan in place (refer to heading Particular Vulnerabilities as a Hazmat Offeror or Carrier).
3. Detonated, released or otherwise used in the U.S. – These include better collection and sharing of intelligence about terrorists and their plans, better CBP immigration procedures aimed at preventing the entry of terrorists, and generally improved law enforcement at all levels of government.
4. Effective if used (*i.e.*, mitigate their effect) – Generally improved emergency response procedures at all levels of government and public education how to implement protective measures, how to react and respond, etc.

All of us involved in cargo transportation must become more aware of what is being transported. Information about dangerous goods shipments must be safeguarded,

and more care must be given to physically secure dangerous goods in our custody. The ability to recognize suspicious transportation conveyances is crucial.

Most of all, since the terrorist threat is first and foremost from *people*, we must know how to recognize and report suspicious people, behavior and communication, and limit access to cargo and information to those who have been specifically authorized or have a clear legitimate need for such access.

Customs Trade Partnership Against Terrorism (CTPAT) is a Voluntary U.S. Security Program

U.S. Customs and Border Protection ("CBP") has created a video that introduces the ideas behind the creation of CTPAT and the benefits that it provides to the security of the United States and its trade partners. Please view the video here.

CTPAT is a *voluntary* rather than a mandatory program, so there are no customs regulations or other laws that enforce specific CTPAT requirements. CBP began developing the program in 2002 along with other initiatives designed to "push back cargo security beyond U.S. borders" so that security takes place all along the supply chain beginning at the source." The Security and Accountability for Every Port Act of 2006 ("SAFE Port Act") enacted by congress was the initial statutory framework for the CTPAT program. It was then reauthorized and amended to reflect current industry practices and the global supply chain threat. It requires a biennial review and subsequent revisions of the Minimum Security Criteria ("MSC"), which are the security requirements that must be met to participate.

CTPAT defines the supply chain as everything involved in the creation and sale of a product. That covers everything from getting the raw materials, to the delivery to the end user.

Beginning at the point of origin – where cargo destined for export has been made, assembled, grown and/or packed for export – and ending at the distribution point.

As a member of CTPAT, all of these areas, from beginning to end, must be covered by security related criteria. This can be accomplished one of three ways:

1. through a CTPAT member,
2. an Authorized Economic Operator (AEO) member who has a Mutual Recognition Agreement (MRA) with the U.S., or

3. by due diligence to ensure every business partner who is not a member of one of these programs follows the same criteria (which may be more trouble than switching service providers).

The reason CTPAT has to be so comprehensive is that its scope must extend to all players. Thus, in choosing the 12 entity groups (CTPAT Member Entity Groups) to be included in CTPAT, CBP is trying to capture all of the service providers involved in the supply chain.

Please note: The CTPAT logo itself is trademarked. Only companies that are members of the CTPAT program where a request is submitted and approved may utilize the logo for any reason.

CTPAT Member Entity Groups

CBP has established "Minimum Security Criteria" ("MSC") for each of the twelve different eligible business entity groups in the supply chain that may participate in the CTPAT program. The intent is to help optimize the performance of the supply chain while preventing terrorist infiltration and reducing the risk of the introduction of dangerous elements through cargo loss, theft, or smuggling. The eligible CTPAT entities are:

1. Third-party logistics providers (3PLs) – typically specializing in integrated warehousing and transportation services for cargo destined for the U.S. A 3PL typically has one or two traditional core businesses (e.g., warehousing and distribution, trucking, or perhaps international forwarding), and expands to additional services based on customer demand such as retail order fulfillment, pick and pack, through intermodal transportation, cross-docking, inventory or supply chain management.
2. U.S. consolidators – includes air freight consolidators/forwarders, ocean transportation intermediaries (ocean freight forwarders), and non-vessel operating common carriers (NVOCCs) with a business staffed in the U.S. Consolidators combine multiple separate consignments into a single lot or container load which creates a more economical shipping unit to move through transportation segments.
3. Licensed U.S. Customs Brokers – A licensed person or firm in the U.S. who acts as an agent for the purpose of arranging customs clearance, payment of duty, or in-bond transit or re-export of imported goods.
4. Certain Foreign Manufacturers (in Canada and Mexico, and manufacturers in other countries upon *invitation* by CBP)

5. U.S. importers – the person primarily liable for the payment of any duties on the merchandise or an authorized agent acting on his behalf.
6. U.S. exporters – a person or company who sells or ships/delivers goods to a buyer or recipient in another country.
7. Air carriers (airlines) that transport cargo to the U.S.
8. Mexican long haul highway carriers
9. U.S. highway carriers (US, US-MX, and US-CA trucking companies)
10. Rail carriers that transport shipments from Canada or Mexico and have one office staffed in U.S. Canada or Mexico via rail.
11. U.S. Sea carriers (vessel shipping lines) that transport cargo to the U.S
12. U.S. Marine Port Authority and Terminal Operators ("MPTO"s) – a person engaged in the business of furnishing wharfage, dock, warehouse, or other terminal facilities in connection with a common carrier, or in connection with a common carrier and a water carrier. Marine terminal operators can include railroads who perform port terminal services not covered by their line haul rates; common carriers who perform port terminal services; and warehousemen who operate port terminal facilities. This term does not include shippers or consignees who exclusively furnish marine terminal facilities or services in connection with tendering or receiving proprietary cargo from a common carrier or water carrier.

Why do Foreign Suppliers, Transportation Carriers, and Supply Chain Service Providers Join CTPAT?

If U.S. importers and exporters hire business partners such as suppliers, transportation carriers and other supply chain service providers that are direct CTPAT program members, the burden of implementing Minimum Security Criteria (MSC) is significantly reduced. For business partners who are not CTPAT members, it is up to the importer or exporter to ensure the business partner is following applicable MSCs. If the business partners are already CTPAT members then they answer directly to CBP. So CTPAT members want to partner with other CTPAT members. Consequently, foreign suppliers incorporated in Mexico or Canada, carriers and other eligible entities typically join CTPAT to maintain their business relationships or facilitate new business opportunities with CTPAT members.

General Benefits of CTPAT Participation

Member Benefits (courtesy CBP.gov/CTPAT)

As a *voluntary* program, there are no penalties for non-participation or non-compliance. The only sanction consists of being dropped from the program. It takes an investment of time and money to set up and operate under CTPAT. So why should a company want to join CTPAT? Are there tangible benefits that outweigh the costs?

A primary motivation to join CTPAT are the benefits of the program, and in return for these benefits, the company must implement and maintain a variety of supply chain security measures as specified by CBP. All of an importer's import shipments from each foreign supplier become subject to the Minimum Security Criteria (MSC) along the supply chain from the point of foreign shipment to the place of U.S. cargo distribution.

Implementing and maintaining required CTPAT security measures throughout an importer's supply chains is usually a significant effort since there are many players involved. Nobody wants to feel the impact of terrorist activities, but most companies don't feel that is enough motivation to join CTPAT. Operational and marketing benefits are what really drive CTPAT participation. For example, all CTPAT members enjoy these benefits:

- Penalty Mitigation: CTPAT's Trusted Trader status will be taken into consideration and any implemented corrective measures, when mitigating penalties.
- Marketability: Membership in CTPAT can improve company reputation and marketability just like certification with certain U.S. government agencies or participation in the International Standards Organization ("ISO").

The Trusted Trader Program mentioned above involves a unification of supply chain security aspects of CTPAT and the internal controls of the Importer Self-Assessment ("ISA") Program to integrate supply chain security and trade compliance.

CTPAT Security Measures—"Minimum Security Standards"

Early in the program deployment, CBP issued "Minimum Security Standards" (MSC) for each type of CTPAT member, referred to as an "entity". Most of the CTPAT minimum security criteria are the same or quite similar for all types of CTPAT members, with variation primarily reflecting the differences in the supply chain operations and services being performed. However, the 2020 updates are more comprehensive, beginning with the development of twelve categories grouped into three focus areas.

The focus areas are:

- Corporate Security – ensuring that senior management is held accountable for assurance of program implementation. The risk assessment includes criteria on business continuity by establishing a culture of security that exists throughout the company. This is accomplished through a system of checks and balances, cybersecurity protocols, and personnel training on best practices.
- Transportation Security – This area covers the physical movement and handling of goods in the supply chain. These areas include security protocols for import and export processes, secure paperwork, inspection of instruments of international traffic (containers), security seal protocol, and maintaining the security of in-transit cargo. Agricultural security is a new category that falls in this focus area.
- People and Physical Security – This is a more familiar area, such as securing facilities and personnel training. Employee education is a key component and program requirement.

In addition, the changing landscape has created a need for a social compliance program and the addition or improvement in five areas:

1. Security Vision and Responsibility – with support of upper management making security an integral part of company culture
2. Cybersecurity (new)– security of information technology and trade data moving within cyberspace
3. Agricultural Security (new)– protection of the supply chain against agricultural pests and contaminants
4. Prevention of Terrorist Financing - protection against money laundering through trade

5. Security Technology - fortification of security in physical areas by using technology (i.e., security cameras and intrusion alarms)

CTPAT is designed to be flexible, therefore many criteria do not contain specific timeframes for completion. Criteria requiring written procedures assume that the procedures have already been implemented and followed. Each company's business model is different; appropriate security measures must be implemented based on risk. These decisions will be made primarily by management.

What CBP hopes to accomplish by application of these requirements is twofold:

- To help optimize the performance of the supply chain while mitigating the opportunity for infiltration by terrorists.
- Reducing the risk of introducing dangerous elements into the global supply chain through cargo loss, theft, or smuggling.

As part of the decision to proceed with CTPAT participation, senior management must understand and carefully consider the feasibility of meeting the minimum requirements worldwide. To demonstrate that supply chain security is a priority, and to make it the most effective, it must be integrated into the company business process. Senior managers must set an example by becoming involved and delegating the appropriate resources to get the job done.

In considering security measures, it is important to understand that for CTPAT purposes a supply chain is defined from the point of origin (manufacturer/supplier/vendor) through to the point of distribution in the destination country, which means *after* the goods have been cleared through customs and completed the through international transportation.

In simpler terms, the supply chain begins at shipment origin point (manufacturer/supplier/vendor facility) and ends at the through transportation delivery point (distribution point) in the U.S. following customs clearance. With the exception of a manufacturing supply chain in which through import transportation is contracted to the factory that will consume the product in the manufacturing process, the "point of distribution" is typically not the final consumer of the goods.

The criteria are broken out into things that "must" be done, and things that "should" be done. Management will have to decide whether recommended measures are implemented. (Things which are optional now may become mandatory in the future.)

Requirements for CTPAT members may also be required of the members' business partners.

Note: If your company is a CTPAT member that becomes involved with cargo shipments inbound to the U.S., expect certain departments to come under scrutiny as to operational security and specific security measures to be implemented.

CTPAT Focus Areas for All Personnel

This lesson will cover the categories in the three CTPAT minimum security criteria focus areas of Corporate Security, Transportation Security, People and Physical Security. There are two new categories in Corporate Security for the 2019 edition of CTPAT; Security Vision and Responsibility and Cybersecurity, as well as those that were already in play such as Risk Assessment and Business Partner Security. Transportation Security also has four categories; Conveyance and Instruments of International Traffic (IIT), Seal Security, Procedural Security and another new one, Agricultural Security. The focus area of people and physical security encompasses physical access controls, physical security, personnel security and what brought you to this training, education, training and awareness.

CTPAT Corporate Security

Security Vision & Responsibility 1.0

First and foremost, in order for a program like this to remain effective it must have management support. Security must become an integral part of the company's culture and be included in the written policies and procedures companywide.

CTPAT members *must*:

1. Include a written and regularly updated plan within the supply chain security program for periodic review of personnel documenting that the security system is being followed properly.
2. Appoint a point of contact that is knowledgeable about the program's requirements and will keep upper management informed regarding all aspects of the program (i.e., issues, audits, exercises, validations). Know who your point of contact is for reporting issues that you think are relevant. This could be your manager, supervisor or an appointed security compliance person.

The CTPAT members supply chain security program must include a written and regularly updated plan for review of personnel to document that the security system is being followed properly.

Risk Assessment (RA) 2.0

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

The risk assessment is *to analyze external threats against company procedures identifying where vulnerabilities exist and modifying or improving company procedures to reduce that risk*.

These two criteria *must* be completed by CTPAT members

1. Conduct an overall risk assessment of your company's supply chain. The assessment must be two-fold. A self-assessment of policies and procedures within the company, and a geographical assessment of threats based on the company business model and role in the supply chain.
2. Risk assessments must be reviewed annually or more often based on risk factors.

Business Partner Security 3.0

This category covers the requirements that CTPAT member must or should impose on its business partners. CBP defines business partners as *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 direct and indirect) 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* and include:

- Foreign consolidators – this includes air freight consolidators, ocean transportation intermediaries, and non-vessel operating common carriers (NVOCC).

- Customers
- Contractors
- Cargo handlers
- Customs brokers
- Exporters
- Foreign suppliers
- Freight forwarders
- Importers
- Manufacturers
- Transportation carriers– includes air carriers, highway carriers, long haul carriers in Mexico, rail carriers and sea carriers.
- Vendor
- Any other supply chain service provider, including a third party, who will have custody or control of the cargo from the supplier's origin facility through to the point of delivery (distribution) in the U.S.

Encouraging and ensuring that all these players, domestically and internationally, comply with minimum security measures is no small matter. It can become a massive initial undertaking for business partners who are not themselves willing or authorized to directly participate in the CTPAT program. Most foreign suppliers, foreign transportation carriers who do not provide through service to the U.S., and forwarders who do not have offices in the U.S. *cannot* directly participate in CTPAT. So a CTPAT certified company *must* reach out to all these foreign players, communicate the minimum security measures that must be implemented, and then follow up in a variety of ways to assure such measures are in place and are being followed. It is crucial to ensure business partners directly handling cargo or documentation relating to the movement of goods have effective security measures in place.

It takes leverage, influence and follow-through to achieve worldwide supply chain security. Think about the practicalities of a U.S. company requiring foreign suppliers and service providers to meet these measures as you consider them. Also consider the additional layer of complexity and risk when using business partners that subcontract certain functions.

CTPAT members must:

1. Obtain evidence of business partners that are certified in CTPAT or another approved party involved in the international movement of goods like an AEO.
2. Have a written, risk-based process to screen and monitor business partners.

CTPAT members except for customs brokers and marine port authority terminal operators must:

- Outsourcing or contracting requires the CTPAT member to ensure business partners have security measures in place that meet the minimum security criteria.

Cybersecurity 4.0

Cybersecurity is applicable to all companies. As companies increasingly use technology it also impacts the supply chain. The risk of data breaches and cyberattacks has increased considerably. Security for information technology is the defense against intruders and unauthorized access to information which can sometimes be equally as damaging as threats to facilities and cargo. Increased connectivity to the internet also increases the risk that the company's information systems can be hacked. This threatens all companies, from small businesses to large corporations. It has become imperative to implement measures to secure information technology (IT) and data. As companies increasingly use technology it also impacts the supply chain.

Automated systems and networks that store documentation must be subject to IT security policies, procedures and standards. Access must be controlled through individually assigned user accounts that require periodic password changes. Access should be limited to those who have a need-to-know based on job assignment.

Networks are defined as *an open communications medium that allows a number of systems and devices to communicate with each other. A network is a collection of computers and other devices that are able to communicate or interchange information with each other over a shared wiring configuration.*

CBP defines Cybersecurity as *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) is defined as *computers, storage, networking, and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data*.

Every criteria in this category applies to all entities. This is considered a new category in the 2019 edition of CTPAT; however, it is similar to the Information Technology category in the first edition. It has been expanded and strengthened from the first 5 criteria to 13 criteria. Ten criteria are requirements for CTPAT members, the first seven should be expanded to ensure business partners also follow the requirements:

1. Install and update protection from malware, social engineering, and internal/external intrusion. Procedures must include recovery or replacement of systems and/or data.
2. Systems must be able to identify unauthorized access and abuse of policies and procedures with consequences for violators.
3. User access must be restricted based on job requirements, reviewed regularly and removed upon separation.
4. Users must have individually assigned accounts with strong passwords.
5. Employees with a remote connection must access the company intranet securely when outside the office. Procedures must be in place to prevent unauthorized remote access.
6. Personal devices used to conduct company work must adhere to company policies and procedures including regular security updates and secure network access.
7. All IT equipment containing sensitive information regarding imports and exports must be inventoried and properly disposed of.
8. CTPAT members must have a comprehensive written cybersecurity procedure covering all Cybersecurity criteria.
9. Cybersecurity policy and procedures must be reviewed and updated annually at the minimum.
10. Members must regularly test infrastructure security and correct vulnerabilities as soon as possible.

4.2 CTPAT Members Defend Against Common Cybersecurity Threats

Common Cybersecurity Threats

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 other unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.*

A company is required to protect all software and hardware against common cybersecurity threats such as malware and intrusion, viruses, spyware, worms, and trojan horses. Security software must be current and receive regular updates. A firewall must be installed and security software must be installed and receive regular security updates. Policies and procedures must be documented and in place to address and prevent:

- Data breaches
- Loss of data
- Loss of equipment

The protocols and procedures must also address the recovery or replacement of IT systems or data in the event of an attack.

Social Engineering

In the context of information security, social engineering is the use of deception to manipulate individuals into giving out sensitive information. The most prevalent method of attack by social engineering is by e-mail, also known as phishing. Here are a few types of social engineering attacks you may not know about:

- Baiting – When someone intentionally leaves behind physical media, such as a USB drive, possibly with an authentic looking company logo or a label with some sort of report name. They are hoping it will get picked up and inserted into a PC possibly causing malware or a virus to be installed.
- Pretexting – When a hacker tries to get information by pretending to be someone you trust. This can be done in person or over the phone and they most likely already have some information about you and use it to gain your trust.
- Shoulder surfing – when a person hovers over your shoulder to obtain your personal information, such as a password, or a PIN at an ATM.
- Smishing – When hackers send SMS messages and attempt to acquire personal information or send the user to a website that has malware.
- Tailgating – An attacker closely follows behind someone with legitimate access to gain entry into a restricted area.
- Vishing – Like phishing but over the phone.
- Water holing – A hacker identifies a website users visit often, also known as a watering hole. The hacker then tries to find a weakness to inject code that infects the visitor's system with malware.

Social Media

This should go without saying, but NEVER post company documents such as cargo manifests, or shipping information to social media pages like FaceBook, Linkedin, Twitter, blogs. Although people should obviously know better, sensitive information has becom public that way.

Consequences of Unauthorized Disclosure

Disclosure of information to persons who do not have a legitimate need to know can result in very serious consequences, including:

- Job loss – If you are caught inappropriately sharing information to someone who does not have a legitimate job-related need-to-know, you may be subject to disciplinary action or even termination for cause!
- Fines – The government can impose civil penalties up to $10,000 per offence for unauthorized disclosure of certain kinds of information, assessing fines to companies and individuals.
- Lives lost – Information in the hands of terrorists may contribute to a successful terrorist attack, with major loss of lives. Think of how you would feel if you were responsible for disclosing such information!

4.13 Accounting and Proper Disposing of Media, Hardware or other IT Equipment Containing Sensitive Information

4.13 *All media, hardware, or other IT equipment that contains sensitive information regarding the import/export process 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.*

There should be a regular inventory taken of computer media like hard drives, removable drives, CDs, DVDs and USB drives containing sensitive information regarding the import or export process. When taken out of service, they must be properly sanitized and/or destroyed following the National Institute for Systems and Technology (NIST) standards for sanitation and destruction of Information Technology equipment and media.

Proper disposal of materials containing company information is just as important as other safeguard measures. Data on computer disk drives, smart phones and portable media must be either:

Permanently erased - (not merely sent to "trash" or "deleted" from "trash", which merely changes or removes the visible index path to the data), or

Physically destroyed - The device (*e.g.*, a floppy drive) must be destroyed in such a way that the data cannot be recovered

Today's portable media is very convenient for backups and transferring information, but it presents a significant security vulnerability.

- Thumb drives and memory cards – The problem is that these items are easily misplaced, and even when a compelling reason exists to use them (*e.g.,* to temporarily transfer a PowerPoint presentation), too often they are not promptly erased or destroyed.

  If any type of "pocket" media is to be used for other than very temporary purposes and immediately erased, it must be stored in a locked secure place within a secured facility.
- Laptops and office PCs – How many times have people had their laptop stolen or simply left it behind where it cannot be retrieved? It happens, and even though there may be a password on one's user's account, a hacker can easily get past this and read anything on the disk drive. A desk computer at your place of work may be vulnerable to unauthorized use by others, with all your data accessible, if you do not log off when away from your desk! And home PCs are often at even greater risk of unauthorized access or theft. Company information should only be kept on computers that are subject to good physical access controls and login discipline.

- Smart phones & PDAs –
  These extremely helpful multi-purpose devices are also mass data storage devices, and at high risk of being lost, stolen and even remotely hacked. Avoid storing company information on these devices.

Information becomes ***YOUR responsibility.*** Be careful to return it to the person who provided it or destroy it when no longer needed.

Conveyance and Instruments of International Traffic Security 5.0

Throughout this section we will be using the term container and Instrument of International Traffic (IIT) interchangeably. CBP defines Instruments of International Traffic (IIT) as *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*.

Most of the non-bulk cargo enters the U.S. in some type of container. Once loaded, these containers move by land transportation to the port of export to be loaded aboard a conveyance, often being transferred at least once between carriers. Terrorists may target the containers and conveyances at any point in the process. Here are some reasons why:

- They move in large numbers between well-established trading partners. If a terrorist can manage to gain access to a container, the chances of being caught are very low. CBP can only physically inspect 2% and scan another 3% of the cargo coming into the U.S.
- They have the capacity to carry just about anything a terrorist might want to ship and the metal walls and surrounding legitimate cargo can help conceal smaller items from inspection.
- They can move from just about anywhere in the world to just about anywhere else.
- Most move predictably. With access to shipper or consignee information, terrorists can work out the container's itinerary (*e.g.,* when the container reaches the origin port, the vessel name and schedule, when it arrives at the destination port, when it is available for customs release, and when it leaves the terminal).

Container traffic, especially shipper-packed through intermodal movements, are of great security concern. Cargo at rest is the least controlled and more vulnerable to tampering. Seal controls and methods to track cargo and conveyances in transit are key measures to prevent the introduction of unauthorized material or persons. The following CTPAT criteria are designed to prevent terrorist access to shipments at the point of origin and en route to origin ocean ports, and to detect container intrusion and tampering long before cargo reaches the U.S.

There are a total of thirty criteria in this category but only two of them apply to all entities:

1. Everyone, CTPAT members and their business partners, must store conveyances and instruments of international traffic securely to prevent unauthorized access.
2. If a threat to the security of a shipment or conveyance is credible or detected, CTPAT members must alert all business partners in the supply chain that may be affected, and must notify law enforcement as necessary.

The following links have been provided by CBP to assist in the reporting of security incidents and suspicious activity. Please make a note of them in case they are needed in the future. :

- ICE Tip Form – to report suspected criminal activity, including money laundering, human and narcotics smuggling, trade export and/or import violations, terrorism, and cybercrimes
- Human Trafficking vs Human Smuggling – information on the differentiation between human trafficking and human smuggling and guidelines on reporting these activities
- e-ALLEGATIONS – CBP Portal to report on suspected violations of U.S. Customs Law and related illicit trade activities
- Recognize the Signs of Terrorism-Related Suspicious Activity – an infographic on how to recognize suspicious activities. Part of the "If You See Something, Say Something" campaign.

Seal Security 6.0

Continuous seal integrity is crucial to a secure supply chain. Instruments of international traffic must be sealed properly. Proper fastening of less than truckload shipments is also required. High-security padlocks must be used on local freight when consolidation hubs are not used. The seal/padlock should be placed at the last pickup site before crossing the border.

There is a total of seven criteria in this section. These four are required by all CTPAT members:

1. Have detailed written procedures including seal control at the facility and during transit.

2. Use of high-security ISO 17712 compliant (cable/bolt) seals on shipments going to or coming from the U.S.
3. Seal inventory maintenance must include documentation that that seals meet ISO 17712 standards.
4. Periodic seal inventory audits and documentation by company management or a security supervisor.

Procedural Security 7.0

Procedural security is about documentation and cargo storage and handling requirements. It is essential to have written procedures to maintain uniformity over time. Policies and procedures or guidelines help to mitigate risks. Rules are developed to perform steps that may not be enforced by technical or physical means. CBP defines procedural security as written policies put into place to ensure the safety of the entire supply chain.

Regardless of the size of the company, policies are required to control oversights, determine accountability, and for the development of a system of checks and balances. The business model of the company creating the procedures may determine what is covered and how detailed they need to be.

Procedural security is about protecting information about the movement of cargo. Companies must safeguard their stationery and items bearing company logos that could be used by terrorists to steal a company's identity for illegal purposes, posing as a "safe" business partner or CTPAT member. Identity theft doesn't only happen to individuals.

Procedural security also pertains to reporting incidents and notification to law enforcement. Personnel need the ability to identify a threat or security breach. Training employees on what to look for is essential to recognize a problem. Overages and shortages should be reviewed to look for trends or patterns that might reveal a potential security risk within the supply chain. Unusual or unexplained delays on shipments bound for the U.S. could indicate a problem and should be reported. A vital part of reporting is the escalation procedure when a problem is found or when challenging an unauthorized person or other issues.

All CTPAT Members must:

1. Have written procedures for reporting an incident including the internal escalation process.

2. Have procedures in place to identify, challenge and address unauthorized people.
3. Immediately initiate and document internal investigations of security incidents.

CTPAT members, except for customs brokers and marine port authority terminal operators, must:

- Shippers and their agents must accurately report cargo information to the carrier and carriers must exercise due diligence to ensure accuracy. Documents such as B/Ls and manifests must be filed on time with CBP.

Agricultural Security 8.0

This is a new category for the 2019 CTPAT edition. Agriculture is the largest industry and employment sector in the U.S. An introduction of contaminants, pests, or disease could devastate this industry.

Over the past 250 years, non-native organisms have been introduced both accidentally and intentionally. Non-native organisms have caused huge economic losses in the food and fiber industries and in export markets, and have spoiled natural resources and native species' habitats. Hundreds of non-native species are introduced into the U.S. each year, and increases in global trade volumes will only expand and increase these risks.

This is a requirement for all CTPAT members except U.S. Customs Brokers and U.S. Marine Port Authority and Terminal Operators.

CTPAT People and Physical Security

Physical Security 9.0

Physical security is the first line of defense from the threat of crime and terrorism. Physical security measures are usually designed with a layered approach to supplying redundancy. Beginning with the outside perimeter use of intrusion detection and barriers are standard. Security systems can range from things as simple as lighting, locks, fencing, and alarms to more technologically advanced surveillance equipment like CCTV cameras and electronic intrusion detection sensors.

There is a total of 17 criteria in this category. Seven are required by all CTPAT members and their business partners:

1. Use physical barriers (*e.g.*, fencing, dividing walls, etc.) and deterrents that guard against unauthorized access.
2. Man, or monitor gates, doors, and other points of egress through which vehicles and/or personnel enter or exit. A search of persons and property may be conducted, as necessary.
3. Supply adequate lighting inside and outside the facility to include entrances, exits, cargo handling and storage areas, fence lines and parking areas.
4. Have written policies and procedures governing the use, maintenance and protection of any security technology used for physical security.
5. Secure all security technology, equipment, and connections from unauthorized access.
6. When cameras are used, they must cover key import/export cargo areas and be programmed to record at the highest picture quality setting 24/7.
7. When cameras are used, designated personnel must randomly review footage to verify that security procedures are being followed properly. This audit and any corrective action must be documented and kept and be available for a full audit.

Physical Access Controls 10.0

Physical access control is a matter of who, where, and when someone is granted entrance or exit. Physical access controls do the following:

- Prevent unauthorized entry to facilities
- Maintain control of employees and visitors
- Protect company assets
- Regulate the movement of people and products to meet the operational needs of the facility

Access control points can be doors, turnstiles, parking gates, elevators, or other places where granting access can be controlled. Typically, the access point is a door. When a door is locked access is limited to someone with a key.

Electronic locks in some ways are more secure than mechanical locks. Electronic locks can restrict the key holder to specific times or dates of entry and can provide records of entry into specific doors and possibly even be as detailed as knowing the exact person entering. Mechanical keys cannot do any of those things and can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the lock must be re-keyed.

Positive identification of all employees, visitors, service providers and vendors at all points of entry is imperative. In the electronic world, a physical access control system operates when a credential is presented to a reader that sends the credential's information, usually a number, to a processor. The processor compares the number to an approved list and grants or denies access to the area. If access is denied, the door or other control point remains locked. If there is a match between the credential and the access control list, the access point is unlocked, or opened.

A credential can be something known such as a PIN number, something tangible such as an access badge, or some part of the person, a biometric feature. The most efficient system uses a combination of these because a single credential can be passed around, thereby circumventing the access list. In a two-factor transaction, the credential and another factor are needed for access. The second factor can be a PIN, another credential, biometric input such as fingerprints or handprints, or operator intervention.

CTPAT members must:

1. Document procedures for issuance, removal and changing of access devices such as badges, keys, key cards, etc.
2. Perform a photo ID check of visitors prior to admission to the facility. Information and visit details must be recorded in a log. Temporary identification must be supplied and visibly displayed at all times while visiting.

CTPAT members except customs brokers must:

- Provide written work instructions for security guards that are periodically verified by management for compliance through an audit and review process.

Personnel Security 11.0

Most security breaches are caused by people. Many of them are created by internal conspiracies. Employees may be tempted to collaborate to circumvent security. Pre-employment screenings and background checks ensure that prospective employees are qualified to perform the job and that the person being hired has integrity. Having employees and contractors sign a code of conduct helps ensure that they understand the company expectations and acceptable behavior going forward. The code of conduct should also provide penalties and disciplinary procedures for failure to comply. Random checks on current employees also help to deter employees from inappropriate actions. Poor hiring practices can result in security breaches, significant financial losses, and reduced productivity. This is especially true when hiring personnel in sensitive positions such as those directly handling freight in warehouse,

dock, shipping or receiving positions. Sensitive positions can also include mailroom personnel, drivers, dispatch, and security guards.

Education, Training and Awareness 12.0

It is important for employees to know what types of warning signs to look for, when to be suspicious, how to recognize internal conspiracies, how to maintain cargo integrity, and how to spot unauthorized facility access. Training should be conducted on a regular basis and a record of training should be kept for each employee. Security measures need to be tested to see if they are effective. Emergency procedures need to be tested and drilled so that everyone knows what to do if a real incident happens.

These criteria can also include training business partners who are not CTPAT members on proper security measures to meet the needs of the CTPAT certified company. Incentives for employees are suggested to encourage reporting of anomalies and recommending ways to improve company security.

The following criteria are *required* by CTPAT members and their business partners:

1. *All companies* must establish a threat awareness program maintained by security personnel.
2. *All personnel* must be trained to recognize, and report threats posed by terrorists, contraband smugglers, or illegal activities which may occur at any point in the supply chain.
3. *All personnel* must be trained on how to report security incidents and suspicious activity.
4. *Based on job function,* personnel must be trained on company cybersecurity policies including the need to protect login information and computer access.
5. *Based on job function,* personnel must be trained in the operation and management of specific company technology. Prior knowledge of similar systems and self-training are acceptable.

Summary of Required Security Measures for All CTPAT Members

To summarize the CTPAT Security Measures-"Minimum Security Standards", set the following criteria for all CTPAT members:

Written procedures:

- An up-to-date review of all personnel as outlined in the security program to ensure requirements are followed properly.

- A risk-based procedure to screen and monitor business partners.
- Comprehensive written cybersecurity policies and/or procedures to protect information technology systems and cover all of the CTPAT cybersecurity criteria. Must be reviewed annually or more frequently based on risk.
- Detailed procedures covering seal control at the facility and during transit.
- Procedures for reporting incidents and escalating incident reports.
- Procedures to identify, challenge and address unauthorized people.
- Initiate and document internal investigations of security incidents.
- Policies and procedures governing the use, maintenance, and protection of any security technology used for physical security.
- Procedures for issuing, revoking, and changing of access devices such as badges, keys, or key cards.

Member and business partner audits:

- The CTPAT member must conduct an overall risk assessment of the company's supply chain both an internal company assessment and an external geographical assessment of threats based on the company business model and role in the supply chain.
- Risk assessments must be reviewed annually, or more often based on risk factors.
- Obtain evidence that business partners are certified in CTPAT or an approved Authorized Economic Operator (AEO).
- Security supervisors or management must conduct periodic seal inventory audits to confirm that seals on conveyances and IIT match the logs and shipping documents. ISO 17712 standard seal documentation must be verified during audit and the audits must be recorded.

Computer, Network and Electronics:

- Install and update protection from malware, social engineering, and intrusion and maintain procedures for recovery or replacement of systems and data.
- The CTPAT member must regularly test their IT infrastructure security and correct vulnerabilities as soon as possible.
- Systems must be able to detect unauthorized access and abuse, and there must be documented procedures that cover consequences for violators.
- User computer access must be restricted based on job requirements, reviewed regularly, and revoked upon separation.
- Users must have individually assigned computer accounts secured with strong authentication.

- Employees using a remote connection must access the company intranet securely when outside the office. Procedures must be in place to prevent unauthorized remote access.
- Personal devices used to conduct company work must adhere to company policies and procedures including regular security updates and secure network access.
- All IT equipment containing sensitive information regarding imports and exports must be inventoried and properly disposed of.

Operational requirements:

- The member's CTPAT point of contact must be knowledgeable about the program's requirements and keep upper management informed regarding all aspects of the program.
- Conveyances and Instruments of International Traffic (IIT) must be stored securely to prevent unauthorized access.
- If a credible threat to the security of a shipment or conveyance is detected, CTPAT members must alert all business partners in the supply chain that may be affected, and must notify law enforcement as necessary.
- CTPAT shipments must be sealed immediately after loading with ISO 17712 high security compliant (cable/bolt) seals.
- Use physical barriers and deterrents that guard against unauthorized access.
- Man or monitor gates, doors, and other points of ingress or egress through which vehicles and/or personnel enter or exit.
- Provide adequate lighting inside and outside the facility including entrances, exits, cargo handling and storage areas, fence lines and parking areas.
- Secure all security technology, equipment and connections from unauthorized access.
- When cameras are used, they must cover key import/export cargo areas and be programmed to record at the highest picture quality setting 24/7. Footage must be randomly reviewed by designated personnel to verify that security procedures are being followed properly. This audit and any corrective action must be documented and records must be maintained and be available for a full audit.
- Perform a photo ID check of visitors prior to admission to the facility. Information and visit details must be recorded in a log. Temporary identification must be supplied and visibly displayed at all times while visiting.
- Verify job application information such as employment history and references prior to hiring new employees.

- Employees and contractors must sign that they have read and understood the Code of Conduct outlining the company expectations and acceptable behaviors, as well as penalties and disciplinary procedures for failure to comply.

Training requirements:

- Training to establish a threat awareness program covering all CTPAT requirements maintained by security personnel.
- Training to recognize and report threats posed by terrorists, contraband smugglers, or illegal activities which may occur at any point in the supply chain.
- Training on company cybersecurity policies including the need to protect login information and computer access. (Based on job function)
- Training in the operation and management of specific company technology. Prior knowledge of similar systems and self-training are acceptable. (Based on job function)
- Training on how to report security incidents and suspicious activity.

CTPAT Minimum Security Criteria Specifically Required of U.S. Customs Brokers

In all of the previous lessons we covered the requirements in each category of the CTPAT minimum security requirements and specified the requirements that applied to all member entities of CTPAT. This lesson concentrates on the "must do" areas that are different for each entity, in this case customs brokers. Since customs brokers must also be able to educate importers on their CTPAT requirements, the last lesson following this will focus on the specific differences for importers.

Specific Benefits for Supply Chain Service Providers

To accomplish international trade, exporters and importers hire a variety of service providers. A typical transaction requires multiple transportation carriers and transportation intermediary(s):

- Consolidators – Commonly known as air freight consolidators, ocean transportation intermediary(s), and non-vessel operating common carriers

(NVOCCs). Typically combine multiple separate consignments into a single shipping unit and arrange the cargo transportation on another's behalf, acting as an indirect carrier.

- Customs brokers – As the supply-chain service provider licensed and most directly regulated by CBP, customs brokers play a unique role in the program, not only in filing customs entries but also in advising importers on CTPAT benefits, responsibilities, and application procedures.
- Third-Party Logistics Providers - Handle logistics functions using their own transportation, consolidation, and warehousing assets and resources on behalf of the client company for international cargo destined for the U.S.

Besides the other benefits, supply chain service providers typically join CTPAT for marketing purposes—specifically to retain and attract business from other CTPAT members. As a requirement of CTPAT, they must ensure their non-CTPAT business partners follow the same minimum security measures they follow. Therefore, the CTPAT carrier saves considerable time and expense if their business partners are also members of CTPAT.

To participate in CTPAT, a carrier must:

1. apply *directly* to CBP
2. operationally implement minimum CTPAT security criteria
3. be prepared for CBP to inspect and validate those criteria are met.

Customs Broker's Eligibility Requirements

In order to be eligible for CTPAT, a U.S. customs broker must be licensed and actively engaged in the conduct of customs business within the past year. The customs broker license serial number, and ABI filer code must reflect this activity. The broker must not owe a financial debt to CBP. There must be an office staffed in the U.S. and a company officer must be designated as the primary cargo security officer responsible for CTPAT. The company must demonstrate excellence in supply chain security practices and make a commitment to maintaining the CTPAT supply chain security guidelines as outlined in the "CTPAT-Partner Agreement to Voluntarily Participate." The broker must sign the agreement and provide CBP with a CTPAT supply chain security profile identifying how they will maintain and enhance internal policy to meet the minimum security criteria.

7.26 U.S. Customs Brokers Must Advise Clients to Report Anomalies

7.26 *Consistent with their for hire services,* ***U.S. Customs Brokers*** *must advise their clients of their obligation to report to CBP and/or any other appropriate law enforcement agency of any anomalies. If applicable, Brokers must also advise their clients to make all required modifications so that the correct data is transmitted.*

This particular security criteria applies only to Customs Brokers because they provide a service and advice to their clients. That includes counseling clients that they are obligated to report any anomalies to CBP and law enforcement as appropriate. Brokers must also urge their clients to make any necessary modifications to documentation so that the correct data is transmitted. Not only is this a requirement of CTPAT, it is also in the *Code of Federal Regulations*:

19 CFR 111.39 Advice to client.

a. Withheld or false information. A broker must not withhold information relative to any customs business from a client who is entitled to the information. Moreover, a broker must exercise due diligence to ascertain the correctness of any information which he imparts to a client, and he must not knowingly impart to a client false information relative to any customs business.
b. Error or omission by client. If a broker knows that a client has not complied with the law or has made an error in, or omission from, any document, affidavit, or other paper which the law requires the client to execute, he must advise the client promptly of that noncompliance, error, or omission.
c. Illegal plans. A broker must not knowingly suggest to a client or prospective client any illegal plan for evading payment of any duty, tax, or other debt or obligation owing to the U.S. Government.
d. ***Customs Brokers*** **must be able to explain CTPAT's security requirements to their importer clients, apprise them of critical program developments, and encourage those importers to become CTPAT Members.**
e. Only customs brokers have opportunities to educate the importing community on CTPAT policy including security procedures, best practices, access controls, documentation fraud, information security, internal conspiracies and technologies that seek to improve global supply chain security. Brokers must be able to explain all of the security requirements of CTPAT to their clients, keep them informed of any CTPAT program developments and encourage importers to become CTPAT members. This is why the importer requirements must be included in the study material for Customs Brokers.

Summary of Customs Broker's Required Security Measures

There are special minimum security criteria requirements specifically for U.S. customs brokers. When reviewing these requirements against the requirements for other types of businesses such as consolidators, foreign manufacturers, importers and exporters, we see some differences.

Since customs brokers do not normally play a part in the physical stuffing, loading, transporting or distribution of merchandise, the criteria does not have specific rules applicable to these areas, however, drivers delivering or receiving cargo must be positively identified with a photo identification.

CBP realizes that customs brokers have another significant role, they must gather and communicate information between entities within the supply chain, including CBP. Because customs brokers are communicating frequently with others in the supply chain, the broker's main role is to educate, corroborate, and encourage these companies to strengthen supply chain security by participating in CTPAT and for those who can't participate, ensure that they take measures to be compliant with the requirements in order to be a business partner.

The main features that differentiate the customs broker's security requirements from the security requirements of other types of companies lie with the documentation, transmission of data, and education of the importing community. Customs brokers must educate clients regarding CTPAT security criteria and where to access it, advise and encourage them to join the CTPAT program if they are not already participating.

Business partners are all third-parties within the client's supply chain that the customs broker communicates with, but not the clients themselves. Brokers have to keep a list of these companies and whether they are CTPAT certified or members of another security program such as an AEO.

One of the most important requirements is that quality data is transmitted to CBP so that they have the information to properly screen the cargo for release or require physical examination. This information is one of the major influences in determining cargo risk. That is why the information received must be legible and protected from tampering. The transmission of information must be consistent with the transaction documentation and it must be submitted on time. If the information received from the importer/exporter is incorrect or incomplete, it must be corrected or completed. If there are errors such as overages or shortages that could create a security risk, they must be investigated and resolved based on information provided by the

importer/exporter; or CBP or another appropriate law enforcement agency must be notified.

Customs brokers must train their personnel how to conduct the security and agricultural inspections, how to recognize and report suspicious cargo, and to educate the importing community on CTPAT and encourage participation in the program.

CTPAT Minimum Security Criteria Specifically Required of U.S. Importers

In all of the previous lessons we covered the requirements in each category of the CTPAT minimum security requirements and specified the requirements that applied to all member entities of CTPAT. This lesson concentrates on the "must do" areas that are different for each entity, in this case importers.

Specific Benefits for Importers and Exporters

The U.S. importer and U.S. exporter are the members most essential to the CTPAT program because they are the parties that have the greatest ability to *control* their supply chain, beginning with the selection and negotiation of service requirements with the foreign supplier or importer, through to and including all the service providers needed to deliver the goods to their destination in the U.S. or the foreign country.

The major difference in benefits for importers vs. other service providers is that it has another aspect to its program. It is also eligible for the CTPAT Trade Compliance program. So there is a compliance aspect in addition to the security aspect.

CTPAT uses the definition of "exporter" from the Export Administration Regulations ("EAR"). It is not the U.S. Principal Party in Interest ("USPPI") as defined in the Foreign Trade Regulations ("FTR"). This may cause issues with businesses that use routed exports or arrange transactions so that they are not the USPPI.

For example:

1. An exporter who is responsible for the entire shipment of goods in a container/trailer would be eligible to receive trade facilitation benefits from CBP and from foreign customs officials, assuming there is an applicable mutual recognition arrangement (MRA) in place.
2. Exporters would be eligible for the program due to their exportation of cargo but would not receive trade facilitation if they are only responsible for a portion of the freight (such as in a consolidated shipment) and if the other shippers with commodities in that container are not CTPAT Members.

The primary operational benefit that CBP has offered to importers and exporters in exchange for CTPAT participation consists of significantly fewer customs inspections of their arriving cargo, and front-of-the-line processing when inspections are required. For exporters this is still dependent on the Mutual Recognition Arrangements (MRAs) in place with the countries they ship to.

Customs inspections can delay cargo by several days and also add hundreds of dollars to landed cost in additional trucking and CES operator fees. Such delays and added costs severely impact just-in-time supply chains.

Many importers and exporters have also realized a variety of secondary benefits from the increased supply chain security measures mandated by CTPAT. These include:

- Reduced cargo theft
- Better order and shipment status visibility
- Improved inventory optimization from a more time-dependable supply chain
- Marketing advantages because potential clients are more confident that cargo is secure

CBP is moving toward a more structured system of specific benefits for importers who participate in the CTPAT program. See definitions for:

- CTPAT Tier 1 Benefits – Automatically available to all CTPAT certified importers. Passing a validation is not required. The main benefit is a somewhat lower security risk score, usually resulting in a lower chance of having cargo undergo a customs inspection for security reasons. More benefits are listed in the glossary definition.
- CTPAT Tier 2 Benefits – An importer becomes eligible when it and its supply chain partners have passed CTPAT validations. The main benefit is a further lowering of its security risk score, thereby further reducing the chance of

having cargo undergo a customs inspection for security reasons compared to CTPAT Tier 1 importers.

- CTPAT Tier 3 Benefits – This is the highest level of benefits an importer can receive through participation in CTPAT and is limited to importers whose supply chains, inclusive of foreign suppliers and supply chain providers, have not only passed validation by CBP, but exceed the CTPAT minimum security criteria, and have adopted "security best practices." A Tier-3 importer becomes eligible for "green lane" customs release (no inspection, no wait) at marine terminals which have implemented "green lane" handling.

Eligible CTPAT Tier 2 and Tier 3 exporters currently are only able to receive benefits when exporting cargo to Japan and the European Union but they must ensure that the Mutual Recognition Agreement (MRA) and Program boxes are checked in the CTPAT Portal and a company officer must sign the Exporter Operations Agreement.

Operational benefits vary somewhat by transportation mode. Trucks arriving at a border customs crossing carrying CTPAT cargo are much more likely to get the FAST "green light" and proceed through without having to stop for inspection. Similarly, air cargo and ocean shipment will receive fewer inspections, and ocean shipments from CTPAT importers will get "front-of-the-line" treatment when examinations are required. Tier 3 importers will receive a "green lane" release at marine terminals where it is available.

Note: CBP routinely performs radiation detection and other non-intrusive inspection of intermodal containers at the foreign port of loading or the U.S. port of arrival, and participation in CTPAT does not affect this type of screening.

CTPAT Trade Compliance Benefits for Importers

Trade compliance is the ability of the importer to meet the CBP's and Partner Government Agency's ("PGA") regulatory requirements. What was previously known as Importer Self Assessment (ISA) has fallen under the CTPAT umbrella. The transition of the ISA to CTPAT expands the definition of the program, creating the equivalent of an Authorized Economic Operator (AEO) in the U.S. This part of CTPAT will execute a trusted trader strategy with the goal for members to be able to quantify the value of their participation in the program. This expanded program provides:

- A national account manager (NAM) as a liaison between the company and CBP.

- Application of coverage to multiple business units.
- No longer susceptible to regulatory audit's focused assessments.
- Access to importer trade activity ("ITRAC") data through the CTPAT trade compliance portal.
- Post entry reconciliation flagging up to 60 days prior to liquidation of the underlying entry summary.
- Expedited binding rulings and internal requests to be processed within 20 days of receipt.
- The ability to request transport for "exam on company premises."
- The ability to request cargo manifest confidentiality automatically.
- Exemption from random non-intrusive inspections.
- Protection from the exploitation of identity theft by creating a notification and verification system.

Importer's Eligibility Requirements

In order to be eligible for CTPAT, a U.S. importer or a non-resident Canadian importer must have a valid continuous import bond registered with CBP and have imported into the U.S. in the past year. Their social security number (SSN), Internal Revenue Service (IRS) identification, or a CBP assigned importer ID must reflect this activity. The importer must not owe a financial debt to CBP. They must have an office staffed in the United States, and a company officer must be designated as the primary cargo security officer responsible for CTPAT. The company must demonstrate excellence in supply chain security practices with no significant security-related events. They must make a commitment to maintaining the CTPAT supply chain security guidelines as outlined in the "CTPAT-Partner Agreement to Voluntarily Participate." The importer must sign the agreement and provide CBP with a CTPAT supply chain security profile identifying how they will maintain and enhance internal policy to meet the minimum security criteria.

Summary of Importer's Required Security Measures

There are specific CTPAT requirements for importers in addition to the Summary of "Must Do" CTPAT Security Measures for all.

Where a CTPAT member outsources or contracts other businesses along the supply chain, the member must make sure that these business partners have security measures in place that at least meet the minimum security criteria required by CTPAT. Due diligence to audit companies must take place either by visiting or surveying them. If weaknesses are identified corrections must be made and documented.

Conveyances and containers must be inspected prior to loading. CTPAT requires a 7, 8, 10 or 17 point inspection depending on the conveyance or container. Importers must also inspect the hardware, locking mechanisms, and seals. If any pest contamination is found it must be cleaned up and preventive measures taken. Importers must properly identify and log all drivers that deliver cargo to or collect cargo from the facility with details of their visit. Cargo must be secured from unauthorized access. Any cargo discrepancies must be investigated and resolved.

Importers must have documented procedures for conducting inspections, for preventing pest contamination., and for handling the information used to clear merchandise. Importer policies and procedures must include work instructions for security guards. Shipment documentation must be legible, complete, accurate, submitted on time and also protected from loss or unauthorized access.

Importers must train their personnel on how to conduct the security and agricultural inspections, how to detect and prevent pest contamination, and how to recognize and report suspicious cargo.