CTPAT's Glossary of Terms

July 25, 2018

General Definitions

CTPAT Member – Membership to the program as a *Certified* Member takes place once three critical steps have occurred. First, U.S. Customs and Border Protection (CBP) has determined that the applicant meets all the eligibility requirements for the type of business entity the applicant has applied for (Importer; Customs Broker; Highway Carrier; etc.). Second, the applicant has successfully passed an internal vetting process, which determined that the applicant is in fact a company that may be trusted by CBP based on its history with the agency, particularly the lack of security related incidents associated with the applicant, to include shipments having been compromised with narcotics or conveyances having been found to harbor illegal immigrants. Third, CBP has determined that the applicant meets the program's minimum-security criteria (MSC), as demonstrated by the applicant's description of its security program provided in the CTPAT Portal's Security Profile section.

To maintain Membership status, a company must continue to meet all program requirements, which include adhering to the MSC and maintaining its eligibility status. In return, CBP commits to affording the CTPAT Member certain benefits. This partnership is documented in a Partner Agreement between the Member and CBP. Continued eligibility is based upon maintaining qualifying core business activities. For example, an Importer must continue to import into the United States, and a Highway Carrier must continue to cross-goods internationally. A Member is considered inactive if it ceases its core qualifying business activity for a period of 12 months or more. An inactive Member no longer meets the eligibility requirements of the program.

Business Model – For CTPAT purposes, a business model refers to key characteristics about the business that are considered when determining if the company meets the criteria. Below are some of the factors that comprise a company's business model:

- Role in the supply chain, if it fills multiple roles, type of operations handled;
- Size of the business, how many employees;
- Type of legal entity (corporation versus sole proprietor etc.) and business relationships (subsidiary versus parent or stand-alone operation);
- If Importer/Exporter, types of commodities handled;
- Number of supply chains; and
- Number of partners in supply chains.

Flexibility is a cornerstone of the program, and various approaches/solutions may be used to meet the criteria depending upon the company's business model. CTPAT does not expect a

small family run business to have the same level and type of security as a large multinational corporation—or a Customs Broker to have the same security measures as a Highway Carrier.

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 fulfil 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. Two examples of indirect partners are subcontracted carriers and overseas consolidation warehouses—arranged for by an agent/logistics provider.

Facility – Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land, or it may be a section of land, with minimal or no buildings on it, that is dedicated to store instruments of international traffic (IIT).



Incoterms (International Commercial Terms) – First published by the International Chamber of Commerce (ICC) in 1936, Incoterms provide rules and guidance to the trade community, and are often incorporated into contracts for the sale of goods worldwide. Incoterms are a series of three-letter commercial trade terms associated with the transportation and delivery of goods, which define the respective obligations, costs, and risks involved in the delivery of goods from the Seller to the Buyer. Incoterms clearly show who pays for what and when the financial liability is transferred between parties in case something happens to the goods while in transit.

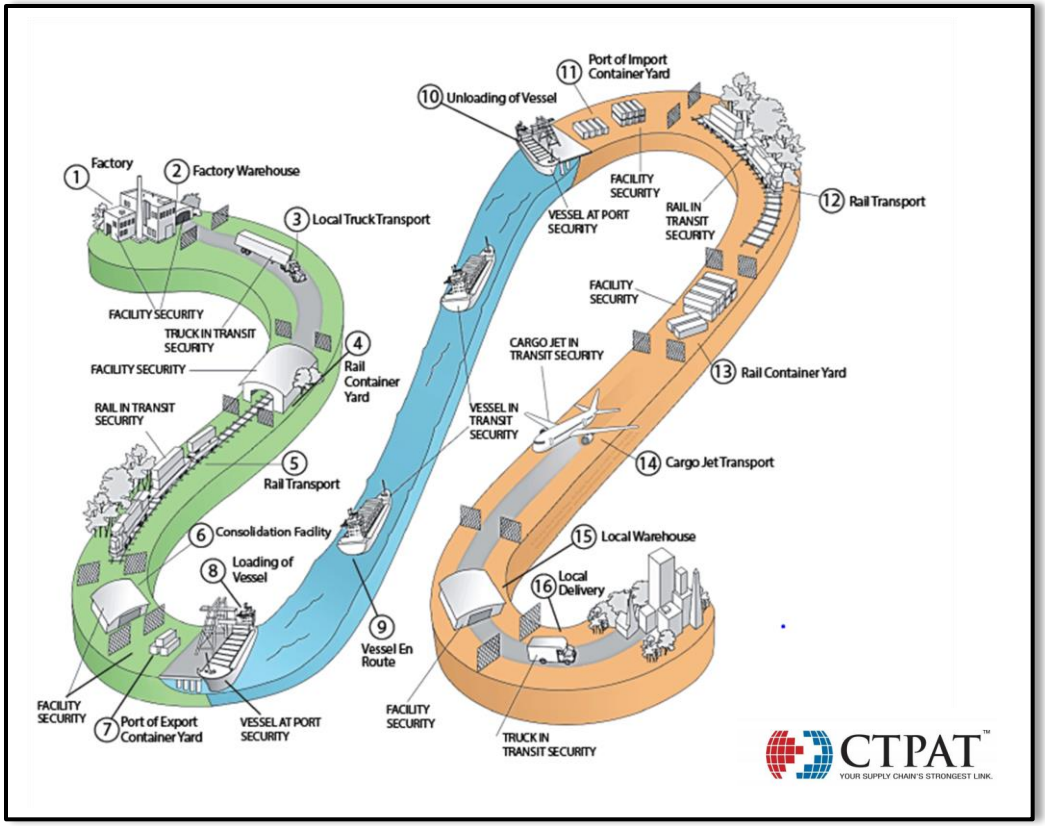
Incoterms have no bearing on security. For CTPAT purposes, what matters is who controls the shipment, which is usually the party that caused the shipment/importation. Regardless of when the Importer becomes the legal owner of the shipment, if the Importer caused the importation to the United States, the Importer is responsible for including this supply chain in its risk assessment.

Point of Origin – Where cargo destined for export to/from the United States has been made/assembled/grown (manufacturer/supplier/vendor) and/or packed for export.

Sensitive Position – 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.

Supply Chain – A supply chain is the network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product, from the delivery of source materials from the supplier to the manufacturer, through to the delivery to the end user. The supply chain for CTPAT purposes is defined from point of origin through to point of distribution.



Conveyance/Instruments of International Traffic (IIT)

Chassis – A special trailer or undercarriage on which containers are moved over the road.

Chassis, Intermodal – A semitrailer of skeleton construction limited to a bottom frame, one or more axles, specially built and fitted with locking devices for the transport of intermodal cargo containers, so that when the chassis and container are conjoined, the units serve the same function as an over the road trailer.



Container, Intermodal – A single, rigid, reusable metal box (capable of being sealed and stacked) in which freight is placed for convenience of movement by various modes of transportation. A container may also have a refrigeration unit, which allows it to be used to transport temperature sensitive cargo.



Conveyance – The powered transport vehicle or unit of a transportation mode, such as an airplane, semi-truck combination, train, or vessel.



Flatbed – An open truck bed or trailer with no sides used to transport oversized cargo, supported by two or more axles; it is used to carry large objects such as heavy machinery, materials, or containers. Flatbeds may have some fixed vertical walls, usually at the front, and may have a variety of moveable stakes, sides, and covers to protect cargo of various types.



Instruments of International Traffic – 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 (CFR, Title 19, Chapter 1, Part 10, Subpart A, Section 10.41a). For Highway Carriers, trailers are to be identified as equipment per Automated Commercial Environment (ACE) manifest requirements.



International Organization for Standardization (ISO) – The ISO is an independent, non-governmental international organization with a Membership of 160 national standards bodies. Through its Members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant international standards; it is the world's largest developer of voluntary international standards. Standards provide requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes, and services are fit for their purpose. ISO International Standards ensure that products and services are safe, reliable, and of good quality.

ISO 17712:2013 – Freight Containers Mechanical Seal – ISO 17712:2013 establishes uniform procedures for the classification, acceptance, and withdrawal of mechanical freight container seals. The ISO Standard provides a single source of information on mechanical seals that are acceptable for securing freight containers in international commerce.

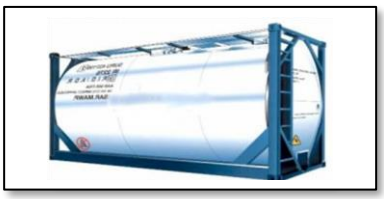
ISO 17712 defines three types of classes of security seal strength, or barrier capacity: "I" for Indicative; "S" for Security; and "H" for High Security. CTPAT requires the use of "H" class seals. Suppliers of seals are also required to use independent third party test laboratories to validate a security seal's classification, and these testing laboratories must also be accredited according to ISO/IEC 17025 (General requirements for the competence of testing and calibration laboratories) to perform testing specific to ISO 17712.

The ISO 17712 standard requires independent testing against the following three factors:

- Physical Strength – Mechanical testing must be conducted to determine a security seals physical strength (Clause 5). - High security seals are manufactured to the highest standards and are marked with an "H" on the seals body. When undergoing mechanical testing by an independent ISO 17025 accredited laboratory (Clause 5) and the manufacturer must be certified to both ISO9001 and ISO17712: Annex A.
- Tamper Indicative Features - Seals must be designed and constructed with tamper indicative features that generate telltale evidence of tampering (Clause 6).
- Manufacturer's Security-Related Business Processes (Annex A) – Poor security-related practices can undercut the effectiveness of a high-quality security seal. ISO 17712's Annex A defines over two dozen required practices, such as facility risk assessments and access controls to production and storage areas. Suppliers' conformance with Annex A should also be demonstrated through an independent certification provider that is accredited to audit compliance with the ISO standards.

In trying to get access to a sealed container, criminal organizations often disregard the seal itself and instead attack the vulnerable parts of the container doors. This tactic allows the bolt seal to remain intact without generating any telltale signs. CTPAT strongly recommends the use of high security cable seals that seal and lock both container doors simultaneously, requiring two cuts for the seal to be removed.

ISO Tank – An ISO tank is a tank container which is built to the International Organization for Standardization (ISO) requirements. ISO tanks are designed to carry liquids in bulk, both hazardous and non-hazardous.



Tractor – A vehicle with four or more wheels designed and used primarily for drawing other vehicles such as a trailer or semi-trailer and not designed to carry a load itself other than part of the weight of the vehicle and load being drawn.

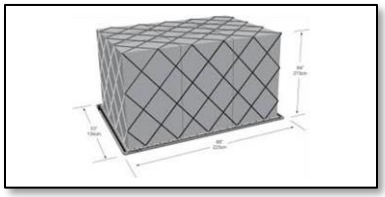


Trailer (Dry Van or Refrigerated Trailer) – A non-motorized cargo container with an attached base or chassis, supported by one or more axles located towards the rear of the container and designed to be drawn by a motorized vehicle such as a tractor. The addition of a refrigeration unit allows the trailer to transport temperature sensitive cargo.



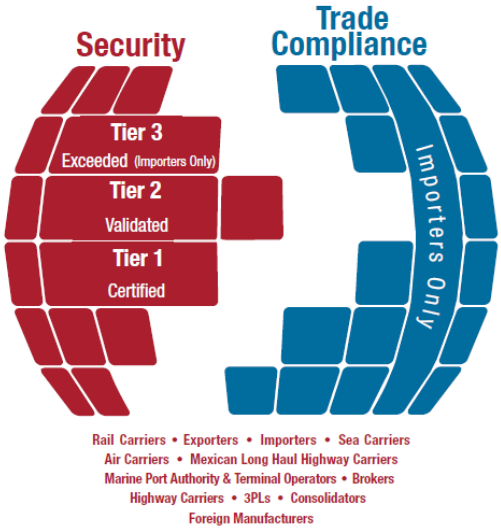
Unit Load Device (ULD) – Any type of container or pallet used to load or transport cargo in the hold of an aircraft.





CTPAT

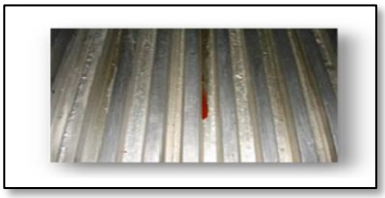
YOUR SUPPLY CHAIN'S STRONGEST LINK.



Agriculture Definitions

Contaminants – Unwanted substance(s) or foreign material in a physical body or in the natural environment that can cause serious harm to U.S. agriculture and its natural resources. Contaminants include soil, manure, seeds, and plant and animal material, which may harbor invasive pests and diseases.

Tire contaminated with manure.



Container with animal blood.

Soil contamination in carrier

Garbage – 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 generated onboard conveyances arriving from any place outside the continental United States, except Canada, is subject to requirements and safeguards for handling once in the United States. The importation of garbage from all foreign countries (except Canada) is prohibited except as provided in 7 CFR 330.401 and 9 CFR 94.5 (c).

Hitchhiking Pests – Pests found with commodities but not generally known to be hosts for the pest; i.e. the pest does not feed on the commodity. Hitchhiking pests may also be found on carrier conveyances where no hosts exist. Pests may simply "hitch" a ride on the carrier conveyance because at some point in the supply chain the conveyance was near or on a host. Examples of hitchhiking pests include snails, bees, grass hoppers, and Asian gypsy moth egg masses.

Snails

Grass Hopper

Asian Gypsy Moth Egg Masses

International Plant Protection Convention (IPPC) – Part of the United Nations' Food and Agriculture Organization (FAO), the IPPC is an international treaty that aims to secure coordinated, effective action to prevent and to control the introduction and spread of pests of plants and plant products.

The Convention extends beyond the protection of cultivated plants to the protection of natural flora and plant products. It takes into consideration both direct and indirect damage by pests, so it includes weeds. It also covers vehicles, aircraft and vessels, containers, storage places, soil and other objects or material that can harbor or spread pests. https://www.ippc.int/en/.

Invasive Species – Insect or plant species that are not naturally found in an environment, and, if introduced, would establish and reproduce to the detriment of naturally occurring species or agricultural production.

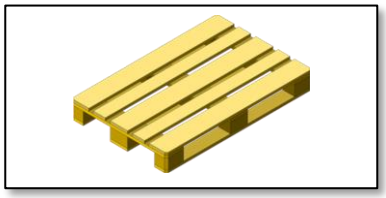
Asian Longhorned Beetle.

Cogon Grass

Khapra Beetle Larvae

Pests – Any species, strain or biotype of plant, animal, or pathogenic agent injurious to plants or plant products. (Source: *United Nations/Food and Agriculture Organization/International Plant Protection Convention (IPPC).*

Wood Packaging Materials (WPM) – Wood or wood products (excluding paper products) that are used for supporting, protecting, or carrying cargo, but not limited to dunnage, crating, pallets, packing blocks, drums, cases, and skids. (Source: *United Nations/Food and Agriculture Organization/International Plant Protection Convention (IPPC).*



Contamination – Visible forms of the following:

- Animals: Insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts);
- Any organic material of animal origin (including blood, bones, hair, flesh, secretions, and excretions);
- Viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, and bark); or
- Other organic material, including fungi, soil, or water—where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).

(Source: *International Maritime Organization/International Labor Organization*).

Cybersecurity Definitions

The source of many of the following definitions is the U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC), United States Computer Emergency Readiness Team (US-CERT) - https://www.us-cert.gov/

Backup – Copying files and applications made to avoid loss of data and facilitate recovery in the event the original is destroyed or compromised.

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.

Electronic Information System – Any hardware, software, media or network, including non-Partner owned devices used to originate, store, process, display, print, or transmit Partner information in electronic form, including, but not limited to mainframe computers, cloud-based computing environments, mini-computers, hand-held computers, personal workstations (PCs), computers, tablets, smart phones, portable storage devices, electronic printers, facsimile machines, telephones, voice mail, email, wireless devices including wireless networks, audio/video devices and audio/video conferencing equipment, and their associated operating systems, support software and application software.

Encryption – The process of cryptographically converting plain text electronic data into a form unintelligible to anyone except the intended recipient.

Firewall - Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network. Firewalls can be configured to block data from certain locations or applications while allowing relevant and necessary data through.

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

Malware – Short for "malicious software," it refers to a type of computer program designed to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Malware can infect computers and devices in many ways and comes in many forms, including viruses, worms, Trojans, and spyware.

Multi-Factor Authentication (MFA) – MFAs can assist in closing network intrusions exploited by weak or stolen credentials. Poor authentication mechanisms are a commonly exploited vector of attack by adversaries. MFA can assist in closing these attack vectors by requiring individuals

to augment passwords, "something you know," with "something you have," such as a token, or "something you are," such as a biometric.

Network – 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.

Passphrase – A passphrase is a memorized secret consisting of a sequence of words or other text that a person uses to authenticate their identity. A passphrase is similar to a password in usage, but is generally longer for added security.

Password – A type of authenticator comprised of a character string intended to be memorized or memorable by the subscriber, permitting the subscriber to demonstrate "something they know" as part of an authentication process.

Patch – A modification to software that fixes an error in an application already installed on an electronic information system, generally supplied by the vendor of the software.

Personal Identifiable Information (PII) – This is defined by the U.S. Department of Homeland Security as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether that individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor. PII may be recorded in any form and it includes name, address, identification number (like a social security number), or factors relating to an individual's physical, physiological, mental, economic, cultural, or social identity (marriage record, credit history, criminal record, marriage record, etc.).

Phishing – A form of social engineering in which attackers use e-mail or websites to solicit personal information by posing as a trustworthy organization.

Portable Electronic Information Systems – Electronic Information System that can be easily moved from place to place, or is expected to be transported during normal usage. This includes, but is not limited to smart phones, tablet computers, ultra-mobile PCs including laptops and notebooks, wearable computers, digital media players, and portable storage devices.

Ransomware – Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software. Phishing emails are crafted to appear as though they have been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, your computer may become infected with malware.

Recovery – The actions necessary to restore a system and its data files after a system failure or intrusion.

Sensitive Personal Information (SPI) – SPI is personal information that could, if exposed, result in possible harm, embarrassment, identity theft, or regulatory, contractual, or policy violations. It includes an individual's social security number, credit or debit card numbers, account numbers, driver's license number, and information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union Membership, or sexual orientation of an individual.

Spyware – A type of malicious software that collects information from a computer system without the user's consent. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information. The data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute financial crimes or identity theft.

Software installed after the user has read and agreed to a clear privacy policy or to an End-User License Agreement (EULA) that describes the software's data collection activities *does not* meet the definition of spyware. It is the responsibility of the user to carefully read such polices and agreements to make sure he/she understands and agree with the terms.

Social Engineering – An attack perpetrated through human interaction (social skills), which relies heavily on manipulating people into breaking security standards in order to gain access to IT systems, networks, or physical locations. The attack may involve direct contact with a person or be indirect via email or other methods.

An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repairperson, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Social Engineering attacks can take many forms such as baiting, phishing, or vishing (the telephone equivalent of phishing). It may be the first line of attack allowing systems to be infiltrated through malware and/or provide access needed to steal company information.

Trojan Horses – A Trojan horse is a computer program that is hiding a virus or other potentially damaging program. A Trojan horse can be a program that purports to do one action when, in fact, it is performing a malicious action on your computer. Trojan horses can be included in software that you download for free or as attachments in email messages.

Virtual Private Network or VPN - A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection and access control.

Virus – A program that spreads by first infecting a computer's system files and then making copies of itself. Allowing it to spread across multiple systems. A computer virus can display a message, erase files, subtly alter stored data, or crash a hard drive. Viruses used to be spread when people shared portable media; however, today, viruses are primarily spread through email messages. Unlike worms, viruses often require some sort of user action (e.g., opening an email attachment or visiting a malicious web page) to spread.

Worms – A worm is a type of virus that can spread without human interaction. Worms often spread from computer to computer and take up valuable memory and network bandwidth, which can cause a computer to stop responding. Worms can also allow attackers to gain access to your computer remotely.

Non-IT Security Technology Definitions

Closed Circuit Television Cameras (CCTV) – Also known as "video surveillance", CCTV is the use of video cameras to transmit a signal to a specific place (a monitor). It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring, such as a loading yard at a manufacturing facility.

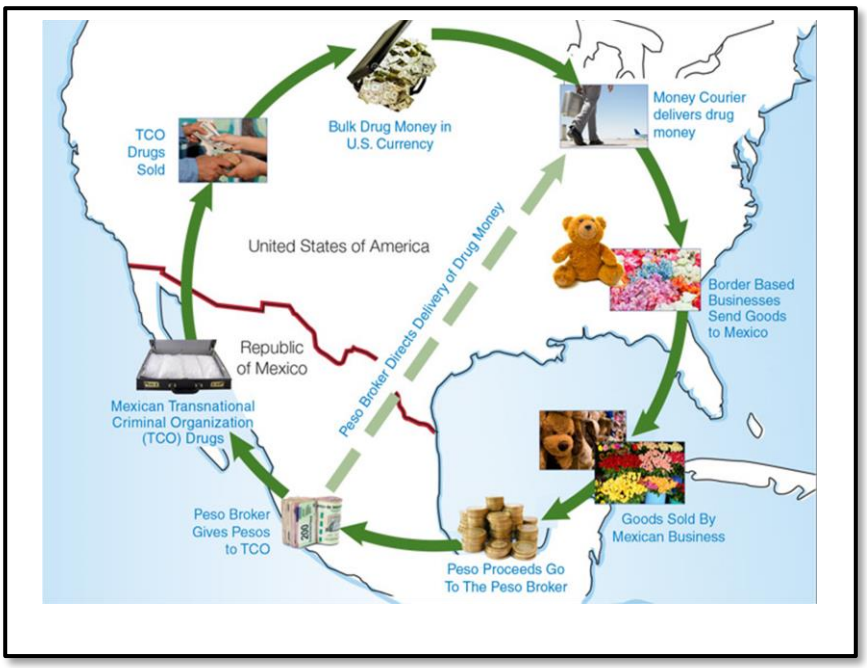
Video Monitoring Equipment - Essentially the equipment used to capture video images transmitted by CCTV technology. There is a variety of means of capturing video footage, to include video tape, digital, disc, and network recordings. Video monitoring can also be performed remotely, via an Internet Protocol (or IP) camera system. An IP camera is a type of digital video camera commonly employed for surveillance, and which, unlike analog closed circuit television cameras, can send and receive data via a computer network and the Internet.

Monitoring Station – Also known as, the "central station," a monitoring station is the principal location where all intrusion detection technology is typically monitored. Some facilities are large enough to monitor their own intrusion detection devices, but the vast majority of those that employ this technology have their intrusion detection functions monitored from a location outside of their boundaries.

Risk Assessment, Money Laundering and Terrorism Financing Definitions

Anti-Western Terrorism – Terrorism is the unlawful use of force against persons or property with the intent to intimidate or coerce a government or civilian population (or sections thereof) in furtherance of a political goal. The explicit targeting of civilians in order to create fear distinguishes terrorism from warfare. Anti-Western terrorism is the use of such tactics against governments or people associated with the United States, Canada, Western Europe, Australia and New Zealand.

Money Laundering – The concealment or disguising of the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. It is the means by which illegally obtained proceeds (i.e., "dirty" money) are made to appear legitimate or "clean."



OFAC/Denied Party Screening – The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals. These sanctions are levied against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

Resilience – The ability to prepare for, adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Examples of resilience measures include:

- Developing a business continuity plan;
- Having a generator for back-up power; and
- Using building materials that are more durable.

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.

Risk Assessment – CTPAT requires its Members conduct an overall risk assessment (RA) based on the Member's role in the supply chain. The RA is made up of two key parts: a self-assessment and an international risk assessment.

The self-assessment (or a security self-assessment) is an internal review/audit of a company's security program against the CTPAT program's minimum security criteria to determine if the company is meeting the program's requirements. The international risk assessment, on the other hand, examines security threats and vulnerabilities associated with a CTPAT Member's international supply chain, from the point of origin where the goods are packed/stuffed for export, until they reach their final destination for distribution.

For further guidance, please consult *CTPAT's Five-Step Risk Assessment,* which is available on the CTPAT website at cbp.gov/ctpat. The five steps in this guide are below:

1. Mapping Cargo/Data Flow and Identifying Business Partners (whether direct or indirect);

2. Conducting a Threat Assessment focusing on, Terrorism, Contraband Smuggling, Human Smuggling, Organized Crime, and conditions in a country/region, which may foster such threats;

3. Conducting a Vulnerability Assessment in accordance with CTPAT's Minimum Security Criteria;

4. Preparing an Action Plan to address vulnerabilities; and

5. Documenting how Risk Assessments are conducted, to include a periodic review of the process.

Risk-Based Approach to Security – CTPAT endorses the application and implementation of security measures based upon a CTPAT Member's own risk analysis. In using a risk-based approach, if a Member determines that one of its business partners or supply chains is of higher risk than others, a greater level of security is necessary. The importance of a risk-based approach is to ensure that security measures to prevent or mitigate supply chain disruptions are commensurate to the risks identified.

CTPAT's goal is to partner with the trade to secure the international supply chain and increase border security. As such, geographical threats (point of origin and in-transit), and business partners' Minimum Security Criteria (MSC) vulnerability are critical factors.

Members need to assess all relevant threats to their supply chains based on indicators such as the complexity of the supply chain itself (number of business partners along the supply chain/length of time cargo is at rest, etc.), presence of terrorist or drug trafficking organizations in the source or transit countries, and history of cargo disruptions (such as evidence of tampering, cargo theft, or contraband introduction).

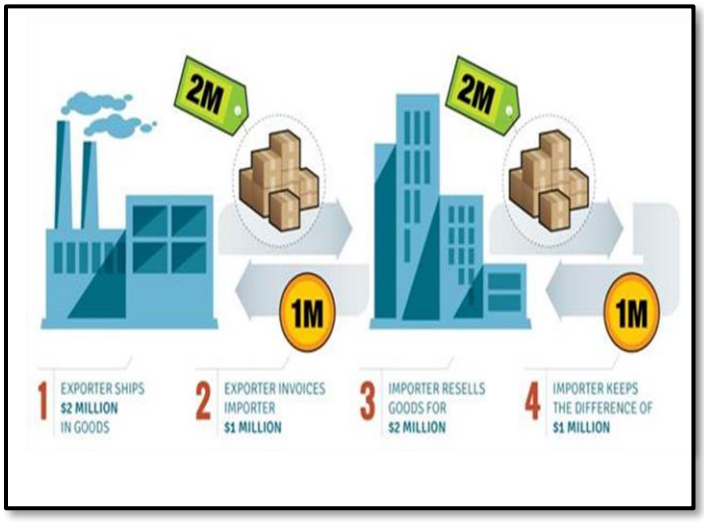
The second step in determining a Member's level of risk includes assessing a business partner's vulnerability with the MSC**.** Vulnerabilities exist when gaps in business partners' compliance with the MSC exist and remain uncorrected. Examples include a business partner's failure to conduct the seven-point container inspection prior to container stuffing/loading, or failure to properly vet third-party vendors.

A risk-based approach can only be achieved by combining a threat assessment with an assessment of business partners' vulnerabilities. Simply noting that a specific country is high-risk for contraband introduction without assessing the business partners' vulnerability and compliance with the MSC does not constitute a risk-based approach.

Supply Chain Terrorism – The unlawful use of force against persons or property with the intent to intimidate or coerce a government or civilian population (or sections thereof) in furtherance of a political goal or for economic gain. Supply chain terrorism is the use of such tactics against any part of the supply chain, including air, rail, truck, or sea transport. It also includes infrastructure such as oil and gas pipelines.

Threat – The intention and capability of an adversary to initiate an undesirable event. Threats should be identified but they are often outside one's control. One cannot prevent a hurricane or a violent demonstration, for example.

Trade-based Money Laundering – An alternative remittance system that allows illegal organizations the opportunity to earn, move, and store proceeds disguised as the proceeds from legitimate trade. Value can be moved through this process by false-invoicing, over-invoicing, and under-invoicing commodities that are imported or exported around the world. Criminal organizations frequently exploit global trade systems to move value internationally by employing complex and sometimes confusing documentation associated with legitimate trade transactions.



Un-manifested Cargo Introduction – Exposure that reflects the threat posed by the introduction of contraband into legitimate cargo in a given country. Evaluations of the threats of un-manifested cargo should consider a country's drug smuggling, weapons smuggling, and stowaways. Un-manifested cargo refers only to the threat of initial introduction of contraband into legitimate cargo, not the transshipment of contraband through a country.