

5-Step Risk Assessment

CTPAT™

YOUR SUPPLY CHAIN'S STRONGEST LINK.

U.S. Customs and Border Protection



5-Step Risk Assessment

Table of Contents

5-Step Risk Assessment Introduction 2

5-Step Risk Assessment Guide 3

Components of the 5-Step Risk Assessment 3

Security Risk Rating 6

Step 1: Mapping Cargo Flow and Identifying Business Partners 6

Step 2: Conducting a Threat Assessment 7

Step 3: Conducting a Vulnerability Assessment 8

Vulnerabilities for Other Entities (Non-Importers) 10

Step 4: Preparing an Action Plan 10

Step 5: Documenting the Risk Assessment Process 11

5-Step Risk Assessment Introduction

The Customs Trade Partnership Against Terrorism (CTPAT) program is one of the primary layers in the multi-layered defense strategy that U.S. Customs and Border Protection (CBP) deployed after the 9/11 tragedy to protect America and its borders against the threat of terrorism. CTPAT works with its members from the trade community to strengthen international supply chains and improve border security.

The primary method of protecting international supply chains is adherence to the CTPAT minimum security criteria (MSC). The MSC is designed to be the building blocks for foreign manufacturers, logistics providers, carriers, and other entities within supply chains to develop effective security practices to prevent or mitigate the risk of theft and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain.

One vitally important aspect of the MSC is developing and maintaining a risk assessment process to examine the amount of risk in members' international supply chains[1]. This will allow members to better understand their supply chains — to assess where there are vulnerabilities and how to mitigate them. Importers must evaluate all their international supply chains, including both direct and indirect imports. Other CTPAT members are responsible for conducting a risk assessment covering their portion of the international supply chain. To assist members in creating a robust and effective risk assessment process, CTPAT initially published the *5-Step Risk Assessment Process Guide in 2010*, updated it in 2014, and this is the third version.

General Business Risk Assessment Versus a CTPAT Risk Assessment:

When it comes to assessing risk, larger companies may already have a risk management department because there are many types of risk that might disrupt a supply chain such as extreme weather events, civil unrest, or piracy. If a company has a separate risk management department, it may be prudent to roll the CTPAT risk assessment into that pre-existing process. However, the risk management division will need to be educated on how CTPAT views the risk of terrorism, which will differ from the traditional risk management view of it on a macro level, shifting to seeing it at both the macro and micro level looking at preventative measures at individual facilities/areas.

Risks for Incoterms Compared to Risks for CTPAT:

On a smaller scale, general business risks usually considered are for individual shipments and would be focused on theft or loss. A warehouse fire or containers going overboard during rough seas are two examples. Companies mostly offset small-scale losses via insurance which party bears the risk in such scenarios depends on contractual agreements. In international shipments, these may be determined via International Commercial Terms (Incoterms), created by the International Chamber of Commerce (ICC) in 1936. Incoterms define the respective obligations, costs, and risks (for loss/theft etc.) involved in the delivery of goods from the seller to the buyer. For more information on Incoterms, see the *ICC website for Incoterms.*

Footnote 1: *The importer's international supply chain for CTPAT purposes is from point of origin to the first distribution point in the U.S.*

Incoterms may sometimes mistakenly be used for assessing risk in regard to CTPAT. Incoterms may deal with some types of security risks for liability purposes, but they do not eliminate risk as it pertains to CTPAT shipments. For example, some importers purchasing goods under the Incoterm Delivered Duty Paid (DDP) or other similar trade terms may consider these domestic imports because the seller or a third party is the importer of record on the transaction. Determining if this type of shipment falls under the CTPAT risk assessment process depends on if the import is a stand-alone or indirect import.

Responsibilities for Indirect Imports:
The importer will have no substantial involvement in a stand-alone import, and any party may purchase goods from that importation, not just the CTPAT importer. An indirect import is *an importation that would not have happened without the importer's substantial involvement (via purchase orders or other contractual means), and the merchandise may only be sold to the importer. For more information concerning indirect imports, see Attachment A, Indirect Imports.*

Business Partners, CTPAT and MRA/AEO Program Members:
When looking at business partners, one must consider if that partner is either a Certified member of CTPAT or a member of another Authorized Economic Operator (AEO) program from another country that has signed a Mutual Recognition Arrangement[2] (MRA) with CTPAT. Generally, this will mean that the partner may be considered low risk, and the CTPAT member is not required to obtain further information beyond verification of the partner's program status. However, if a business partner has been determined to be low risk, (though uncommon) this does not preclude a member from conducting a more in-depth process to verify its business partner's security procedures if the member has decided it is warranted based on additional factors. CTPAT encourages members to consider the level of risk and to focus efforts on higher risk areas/ partners when developing plans to verify compliance with the MSC.

Members' Self-Assessments and Non-Member Business Partner Assessments:
When assessing risk in its supply chain, a member must look at both its domestic and international operations. The international portion of a supply chain is inherently a greater risk, especially since most business models outsource international operations.

Since many foreign business partners cannot be members of CTPAT, or may not be members of an MRA program, these represent a higher level of risk, and that is why one of the most important criterions is ensuring that business partners meet the criteria.

Footnote 2: *For more information about MRAs, see CTPAT_and _MRAs.*

5-Step Risk Assessment Guide

A risk assessment analyzes external threats against existing procedures to identify vulnerabilities. Once identified, companies need to determine what countermeasures are needed — what procedures to implement or improve to reduce/mitigate the risk. For a brief overview of the risk assessment process, see *Attachment B, 5-Step Risk Assessment Process.*

Though recommended, the 5-Step Risk Assessment is not the only risk assessment method, and it is not necessarily all inclusive of what a risk assessment should contain. Like the rest of the criteria, a risk assessment is not a one-size fits all mechanism, and risk assessment processes will vary based upon the entity type, role in the supply chain, business model, and other factors. If used, members need to customize the 5-Step Risk Assessment process to fit their business.

If members' supply chains involve limited numbers of business partners, and have only a few nodes, their risk assessment may not require such extensive efforts. Conversely, CTPAT understands that some members have numerous supply chains, which may present a monumental task to conduct a comprehensive security risk assessment on all of them. If that is the case, focusing on the supply chains that are of highest-risk first would make the most sense.

If a member needs help with its risk assessment process, contact its assigned Supply Chain Security Specialist (SCSS). If an applicant needs help, contact the CTPAT field office closest to your company Headquarters or main office. Contact information is available on the *CTPAT webpage: www.cbp.gov/CTPAT.*

Components of the 5-Step Risk Assessment

1. Mapping cargo flow and identifying business partners (both direct or indirect)
2. Conducting a threat assessment
3. Conducting a vulnerability assessment
4. Preparing an action plan
5. Documenting the risk assessment process

Security Risk Rating

Each CTPAT member is responsible for establishing its own overall security risk rating system based on its business model. The goal is to have a ranked output to see where your company should focus resources to reduce/mitigate risk. Businesses may use various methodologies for rating risk within their international supply chains. The *5-Step Risk Assessment Guide (5-Step Guide)* uses the following simple risk ratings throughout:

1. Low risk;
2. Medium risk; and
3. High risk.

Step 1: Mapping Cargo Flow and Identifying Business Partners

The cargo flow is one of the most important aspects of the risk assessment process for importers, and it is also important for exporters and foreign manufacturers. For other nonimporters, there may be elements of a cargo flow in a broader sense (e.g., regional routes for carriers) that need to be considered, as well as what business partners are involved in your portion of the supply chain.

The more you know about your supply chain, the better your cargo flow and risk assessment will be. To create your cargo flow, you must look at all parties involved in the supply chain, all the transportation legs, and especially where cargo may be "at rest" since that makes it more vulnerable. Therefore, the cargo flow may also feed into the vulnerability assessment since it may uncover previously unknown weaknesses.

Below is a list of some of the parties in an average supply chain that will need to be included in the mapping process:

- The point of origin (manufacturer or producer);
- Transportation carriers (include all modes);
- Consolidation/storage facilities (warehouses);
- Foreign ports (all modes);
- U.S. Port of Entry;
- Domestic carriers (as applicable, truck drayage/long-haul and/or rail); and
- Distribution centers (first distribution point where international shipments are opened).

Some companies rely on third parties to control much of their supply chain and may lack familiarity with how the cargo moves and who is moving it. If that is the case, see *Attachment C, Aid to Map Cargo Flow*, which has a series of questions to help familiarize a company with its supply chain operations.

To begin mapping a cargo flow, it can be a simple process of writing it out in a word document like *Attachment D, Sample of Simplified Cargo Flow;* it can be compiled in a spreadsheet, table, or a flowchart — or however the member wants to do it. Once you have listed the business partners, how the cargo moves in the chain, and the document flow, you can add more details. When identifying the parties in your supply chain, (if applicable) ensure that any subcontracted third parties are included in the vulnerability assessment. For an example, see *Attachment E, Sample of Mapping Cargo Flow and Partners.*

If feasible, physically follow the cargo as part of the mapping exercise. This may also take place during your validation, but often there is insufficient time to track the cargo. However, it is highly encouraged that the member (or its business partner) undertakes this exercise as part of the risk assessment process. When one follows the cargo and visits all facilities that handle the cargo, there may be some unexpected findings. For example, during a validation, the validation team visited the warehouse where the cargo was stored prior to being sent to the airport. The CTPAT team found that the security measures were very poor, and the company point of contact (POC) was also quite shocked at how the cargo was stored since it was sensitive electronic equipment, and the warehouse had no air conditioning. The POC immediately called his business partner and demanded a new location be selected — one suitable for the cargo type, and with better security measures.

In another validation, the team visited the container storage yard that supplied the factory with empty containers. It was a public yard in a port city. The yard turned out to be a lively spot with zero security measures. No guards were seen, and the walls were in disrepair with gaping holes that allowed anyone access into the facility. A small shantytown had taken advantage of the unfettered access, to include food vendors and various other people milling about the stacked containers.

Since it was an initial validation, the vice president of the importer had joined the validation team. Based on what he saw at the container yard, he made the decision to change the company's business model and move from a third-party arranging shipment to contracting directly with a single shipping line. During the company's revalidation, a second supplier was visited (that also shipped out of that city), and the team toured the shipping line's container yard. It was vastly different from the previous yard, with actual walls, a gate, and restricted access via onsite security guards.

Step 2: Conducting a Threat Assessment

The main threats that CTPAT is concerned with are the following:

1. Terrorism;
2. Contraband Smuggling;
3. Human Smuggling and Forced Labor;
4. Organized Crime; and
5. Conditions in a country/region, which may foster/fund such threats (e.g., political unrest or socioeconomic factors).

Since the transport leg (link) is usually the most vulnerable portion of a supply chain, always research specific threats to transport sectors in the country/region. For example, cargo theft is prevalent in some areas. If a threat is present, research the usual modus operandi (MO), or how the theft is carried out.

There are many open sources, which provide information on threats within the international supply chain, a few are listed in *Attachment F, Resource List.*

After conducting research on the threats in a country/region, assign a threat risk rating. The 5-Step Guide simple risk rating for threats is the following:

1. Low risk—No recent incidents/intelligence/information;
2. Medium risk—No recent incidents/some intelligence/information on possible activity; or
3. High risk—Recent incidents and/or intelligence/information.

A score of three in any of the four main threat areas would deem the supply chain to be high-risk. A sample threat assessment is provided, see *Attachment G, Sample Threat Assessment.*

If not already covered, companies should also include other types of threats and how security procedures might be affected by them such as natural and man-made disasters like hurricanes, earthquakes, or civil unrest.

Step 3: Conducting a Vulnerability Assessment

A vulnerability assessment examines facilities and a supply chain as a whole to find weaknesses in procedures and other areas that might allow terrorists and other criminals to infiltrate a supply chain. For some business partners that are deemed low risk due to CTPAT/MRA membership, *these may be checked off as compliant* — unless there is recent information that might warrant a change in their risk status.

Some companies may want to combine the cargo flow with its threat and vulnerability assessments into a more compact format, for examples *see Attachment H, Sample Cargo Flow and Risk Rating, Manufacturer and Attachment I, Sample Cargo Flow and Risk Rating, Highway Carrier.* Smaller entities with a low threat level may opt for a simplified vulnerability assessment, one that identifies overall vulnerabilities a member is susceptible to based on its role (process) in the supply chain, business model, and what threats it faces. For An example, *see Attachment J, Sample Simplified Risk Analysis for a Broker.*

For importers, more complex supply chains may need an in-depth vulnerability assessment that involves conducting site evaluations of each facility/node in the supply chain, as well as looking at each transport leg (and other processes) to verify that security procedures are followed. This area of the risk assessment overlaps with another portion of the MSC in the Business Partners section, which is to verify business partners meet the CTPAT criteria. Where site assessments are needed, their basis will be the CTPAT criteria because it was designed to mitigate existing vulnerabilities within supply chains. Thus, determining how vulnerable an international supply chain is rests mostly on how well business partners adhere to the CTPAT criteria. It is also necessary to determine if there are any unique elements that may not be covered in the criteria that need to be addressed.

Each partner must be evaluated against all the (applicable) criteria and will need to comply with all required (**musts**) criteria in order to meet the minimum level of compliance required by CTPAT. Since the recommendations (**shoulds**) are not mandatory, if they are followed, these will further increase the level of security. If required criteria are not being followed, this will result in a higher risk rating for the vulnerability assessment, and actions must be taken to bring the business partner into compliance.

CTPAT recognizes that the vulnerability assessment is complex because the criteria is a layered system that is designed to allow one layer to fail and still prevent a breach from occurring because other layers (preventative measures) are still in place.

The 5-Step Guide uses the following risk rating of vulnerabilities for CTPAT criteria:

1. Low risk—Meets all required security criteria (**Musts**);
2. Medium risk—Meets all applicable **Musts** in top tier criteria[3] and most other required criteria.
3. High risk—Does not meet all **Musts** in top tier criteria and/or fails to meet multiple required criteria.

There are a few methods to assess compliance with the criteria; the **best** method is *onsite audits*. However, the most common method is a self-assessment conducted by sending security surveys/questionnaires to business partners that are not eligible or do not participate in the CTPAT program. If used, security surveys must collect all basic requirements. To aid members in completing vulnerability assessments on their foreign supply chains, CTPAT has developed an importer handout for foreign business partners, the *Importer Criteria for NonMember Partners.* It contains all criteria that directly pertain to an importer's foreign business partners. The importer must also consider the process/role performed by the business partner in the international supply chain as identified in the cargo flow (e.g., procurement/purchasing, production, packing, storage, loading/unloading, transportation, and document preparation[4]). Additional questions may be needed based on the role of the business partner. Some facilities will perform multiple processes.

The questionnaire should not use only Yes/No questions; follow-up questions are necessary to get better details concerning their security measures. The survey should also address whether or not a system of checks, balances, and accountability is in place, particularly in key areas of the criteria. Members must exercise due diligence in trying to ensure surveys have as much information as possible.

Once a business partner has shown its compliance with the criteria, it is important to have a **recurring schedule** (per the criteria) to reassess a partner to ensure it is still meeting the criteria; otherwise, a company will not be aware if the business partner begins to slip in its compliance over time. The best method is an onsite audit, but if that is not feasible, the security survey will suffice. To that end, CTPAT has provided an *Audit and Self-Assessment Guide* to help members with designing these procedures.

Footnote 3: *For a definition of top tier criteria, see Attachment K, Definition of Terms*

Footnote 4: *Attachment K, Definition of Terms provides a CTPAT definition for each process.*



Vulnerabilities for Other Entities (Non-Importers)

Most of the 5-Step Guide is aimed at importers since they represent the greatest area of risk. However, other entities within CTPAT must look to see what specific vulnerabilities may exist for their entity type/role in the supply chain. For most other entities, the biggest challenge is a lack of control over many elements in the supply chain. Customers represent a large area of vulnerability. Highway carriers may not be picking up live loads; drivers may not witness cargo loading or sealing of the instruments of international traffic (IIT). Carriers that handle less than trailer load (LTL) or less than container load (LCL) freight have greater risk because there are more unknown elements. CTPAT understands the nature of these supply chains and the limitations that may exist in what can or cannot be controlled. CTPAT expectations for these cases is performing due diligence.

For some examples of vulnerabilities for non-importers see *Attachment L, General Vulnerabilities for Non-Importers.* For highway carriers operating in the land border environment, *Attachment M, Land Border Highway Carrier General Cargo Assessment Worksheet* may help identify susceptible areas.

Step 4: Preparing an Action Plan

Once the information has been gathered from the vulnerability assessment, it must be reviewed, and all identified weaknesses must be recorded in an action plan. The plan must provide corrective measures and follow-up to ensure the actions were completed. In many cases, the plan will be to ensure CTPAT criteria is followed. Evidence of implementation (EOI) such as photographs or written procedures must be provided as proof that corrective measures were taken. The action plan must identify who is responsible for carrying out corrective measures and the timeframe for completion, to include the deadline. For an example of an action plan, see *Attachment N, Sample Action Plan.*

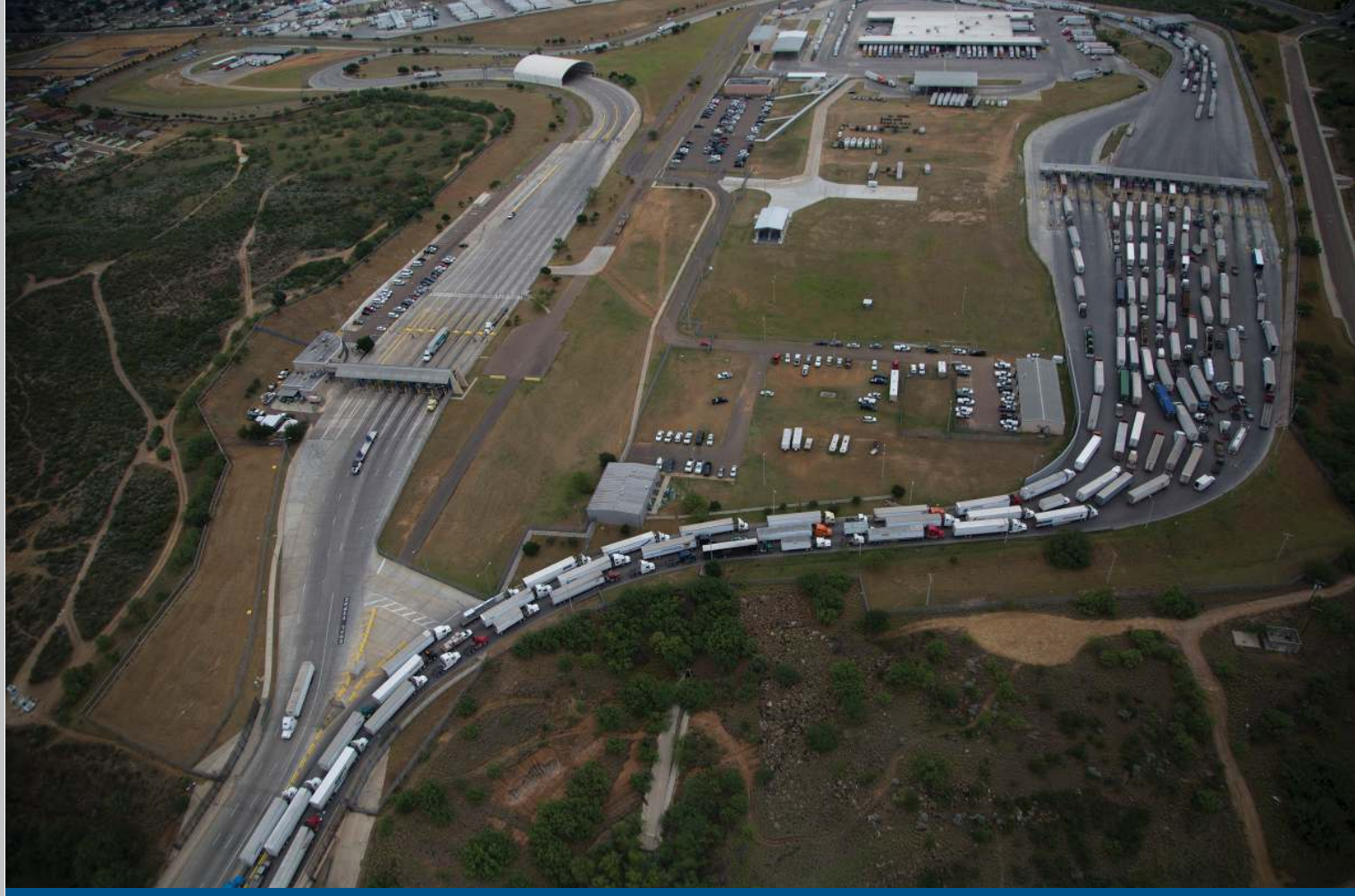
Action Plans for High-Risk Supply Chains

If your supply chain operates in areas with significant (current) threats, and has been deemed high risk, the action plan should consider additional measures. What happens if your supply chain is breached? Ensure procedures for a breach include initial (immediate) steps in the investigation to include notification protocols, interviews of pertinent personnel, and a review of security processes to determine what was exploited to allow it to happen.

Your plan should address specific threat scenarios such as hi-jacking conveyances and kidnapping drivers. Running tabletop exercises or actual mock simulations on the ground to counter specific threat scenarios is useful to help tighten up security measures and ensure employees will follow procedures. Conduct after action analysis of the exercise — what went well, what didn't? Learn from your mistakes. Do you need to change something — implement a new procedure, or is better training needed?

Step 5: Documenting the Risk Assessment Process

A written procedure is needed for how the risk assessment is to be documented to include how often the process is to be reviewed and revised if warranted. For information on documenting a risk assessment process, see *Attachment O, Documenting Risk Assessment Process.*



Index of Attachments for the 5-Step Risk Assessment Guide

Attachment A, Indirect Imports 14

Attachment B, 5-Step Risk Assessment Process 17

Attachment C, Aid to Map Cargo Flow 18

Attachment D, Sample of Simplified Cargo Flow 21

Attachment E, Sample of Mapping Cargo Flow and Partners 22-23

Attachment F, Resource List 24

Attachment G, Sample Threat Assessment 25

Attachment H, Sample Cargo Flow and Risk Rating, Manufacturer 26

Attachment I, Sample Cargo Flow and Risk Rating, Highway Carrier 27

Attachment J, Sample Simplified Risk Analysis for Broker 28

Attachment K, Definition of Terms 29

Attachment L, General Vulnerabilities for Non-Importers 33

Attachment M, Land Border Highway Carrier General Cargo Assessment Worksheet 35

Attachment N, Sample Action Plan 34

Attachment O, Documenting The Risk Assessment Process 35

Attachment A, Indirect Imports

The concept of an indirect import for CTPAT purposes pertains only to security[1] and the risk assessment process. CTPAT considers an indirect import to be merchandise purchased by a CTPAT member, usually through a third party. The third party is the importer of record (IOR) on the entry, and the member is listed as the ultimate consignee (UC). The goods are procured through a purchase order (PO) or similar contractual agreement that usually specifies the Incoterm, Delivered Duty Paid (DDP) or the shipping term, Landed Duty Paid (LDP). In many instances, the UC will consider this a domestic purchase because the ownership of the goods generally does not change hands until the merchandise has cleared Customs in the United States. However, the use of Incoterms or other trade terms deals with the legal aspects of assigning costs, responsibilities, and liability for insurance purposes; they do not pertain to securing a supply chain.

To qualify as an indirect import, the transaction will not represent a stand-alone purchase; the UC must have caused the importation, which means that the import would not have happened without substantial involvement from the UC. To meet the substantial involvement requirement, the import shipment[2] would have to meet at least two of the following conditions:

- The UC is clearly aware that the merchandise will be sourced/manufactured to its requirements and will be imported on its behalf.
- The goods are made to the specifications of the UC, which often include product labels with the UC's name, SKU codes, and/or bar codes. Therefore, no one but the ultimate consignee (UC) could reasonably sell the merchandise.
- There are specific contractual requirements regarding the merchandise or its packaging/labeling.

Having caused the importation to take place, the UC is responsible for ensuring the cargo is secure based on CTPAT's requirements for importers to meet the minimum security criteria.

If the member did not cause the import to take place, that importation will not be considered an indirect import, and its supply chain will not be deemed a part of the member's international supply chain for risk assessment purposes.

Footnote 1: This definition is solely for security purposes as it relates to a CTPAT risk assessment. It does not pertain to regulatory compliance measures nor is it meant to supersede any CBP requirements for the determination of value, preparation of entries, the role of ultimate consignees, and/or the right– to–make-entry provisions etc.

Footnote 2: Importations tied to POs based solely on Just-in-Time inventory practices are not considered substantial involvement, rather a mechanism to control the amount of inventory in the pipeline for the IOR.

For example, a member purchases toys based on a popular movie franchise from a company that holds the license to make the toys. The license holder or licensee manufactures the toys based on the requirements in its licensing agreement with the intellectual property rights owner and imports them from abroad. The licensing agreement does not allow for any changes to the merchandise and includes specifications for the packaging; therefore, the UC cannot include any contractual agreements concerning the goods or the packaging in the PO. All companies that buy the toys from the licensee receive the exact same product. The licensee would be importing the toys regardless of whether it sells them to the UC or another company. As such, there is no substantial involvement from the UC in the purchase of the merchandise, and it is not considered an indirect import.



Attachment B, 5-Step Risk Assessment Process

Step	Process	Description	Methods	Resources
1	Map Cargo Flow and Business Partners	Identify ALL parties involved in the following processes: 1. Procurement/Purchasing 2. Production 3. Packing 4. Storage 5. Loading/Unloading 6. Transportation 7. Document Preparation	1. Request information from supply chain partners 2. Review documentation (Bills of Lading, manifests, invoices, etc.) 3. Determine routing from site visits/audits of the supply chain	See *Attachment E, Sample of Mapping Cargo Flow and Partners*
2	Conduct Threat Assessment	Identify and rate the risk of threat (low, medium, high) for the country and region for each international supply chain, using the following (at a minimum): Terrorism (political, bio, agro, cyber) Contraband Smuggling Human Smuggling Organized Crime Conditions fostering above threats	1. Investigate using open source internet information (government and private organizations) 2. Representative/contacts "on the ground" at Origin should be interviewed 3. Discuss with Law enforcement (foreign/domestic), local state, federal/national 4. Ask if they belong to Trade and security organizations 5. Assigned CTPAT SCSS	See *Attachments F, Resource List* *See Attachment G, Sample Threat Assessment*
3	Conduct Vulnerability Assessment	For all business partners in the international supply chain (directly contracted or sub-contracted): 1. Identify the work function process they perform 2. Verify partners meet applicable minimum security criteria 3. Rate their compliance (low, medium, high)	1. SVI Number/CTPAT Membership 2. Membership in Mutual Recognition Program 3. Ask to see security surveys 4. Site visits by company representative completed? 5. Site visits by overseas personnel/agents? 6. Review Business reports of the company 7. Request their Security certifications covering CTPAT minimum security criteria 8. Ask if 3rd party supply chain security assessments were completed	See document, *Importer Criteria for Non-Member Partners* See *Attachment J, Sample Simplified Risk Analysis for Broker* See document, *Audit and Self-Assessment Guide*
4	Prepare Action Plan	Establish a corrective action plan to address gaps or vulnerabilities found in business partner's security programs.	1. Record weaknesses 2. Identify corrective actions 3. Provide timeline and assign responsibility 4. Verify actions completed	See *Attachment N, Sample Action Plan*
5	Document How Risk Assessments are Conducted	A description of the company's approach, policies, and procedures for conducting an international supply chain security risk assessment.	1. Document company's policy for conducting international supply chain security risk assessment 2. Document procedures to conduct international supply chain security risk assessments	See *Attachment O, Documenting Risk Assessment Process*

Attachment B, 5-Step Risk Assessment Process

Attachment C, Aid to Map Cargo Flow Questions for In-Depth Analysis of Complex Cargo Flows

a. Table of Contents

Number of parties/nodes in your chain: 19

Control of movement of the goods: 19

Packed/stuffed for export: 19

Containment method in transit (instruments of international traffic, IIT): 19

Consolidation/warehousing: 19

Transportation to the Port of Export: 19

Route(s) to the Port of Export: 19

Time/distance between domestic nodes: 19

Freight at rest: 19

Port of Export: 20

Mode of international transport and number of legs: 20

Trading companies/buying agents: 20

Number of parties/nodes in your chain:
- Do you use a freight forwarder to arrange the international shipment of your goods?
- If so, does the freight forwarder subcontract your transportation, or does the company also own a transportation service?
- Are multiple carriers used when transporting goods via trucks, or is it only one carrier?
- Is any carrier allowed to further subcontract? If so, is there proper oversight of the contracted carriers?
- For land border crossings, is there a change of carrier for crossing the border?

Control of movement of the goods:
- What Incoterms/trade terms are used to ship your merchandise?
- What party selects the carrier(s)? Is it your company, the supplier, or a freight forwarder?
- If using a freight forwarder, does the freight forwarder select the carrier for both land and ocean/air? If not, who does?
- If consolidation is performed, who chooses the consolidator?
- The party that controls the movement of the goods has the leverage to ensure security procedures are in place, and it should also be auditing all subcontractors to ensure these protocols are carried out properly.

Packed/stuffed for export:
- Are your goods packed for export at the factory/supplier, or at another facility?
- If packed for export at another location, this information needs to be added to your analysis.
- How long does it take to load an instrument of international traffic (IIT) or conveyance?
- Does the stuffing of an IIT/container ever take multiple days?
- Are containers/conveyances/IIT left overnight or multiple nights at your suppliers?

Containment method in transit (instruments of international traffic, IIT):
- How is your cargo shipped?
- Is it containerized (ocean, rail), via truck, tanker, flatbed, unit load device (ULD), palletized, or loose via bulk shipments?

Consolidation/warehousing:
- If consolidated, is it consolidated with your own merchandise or with goods belonging to other companies?
- Where does the consolidation take place?
- If containerized or shipped via trucks, is your merchandise shipped in full container load (FCL) or full truckload (FCL) or in partial shipments — less than container load (LCL) or less than truckload (LTL)? Or, do you ship via both methods?
- Please note, if you ship merchandise in an LCL/LTL capacity, and it is consolidated with other companies' freight, for CTPAT purposes, it will not receive the same benefits as FCL/FTL cargo.

Transportation to the Port of Export:
- How does your merchandise reach the port of export?
- What mode of transportation is used; is it via rail, truck, feeder vessel, barge, plane etc.?

Routes to Port of Export:
- What route is used to transport the goods to the port of export?
- Is it one set route, or may multiple routes be used?

Time/distance between domestic nodes:
- What are the distances and times involved in transporting the goods to the port from the factory/packing facility?
- If a warehouse or consolidation facility is used, what are the times/distances to and from it?
- Are multiple days involved in the transit of the goods to the port?

Freight at rest:
- Do your goods sit idle while in transit at any point? If so, how many times/places are the goods "at rest" and for how long?
- Are the goods staged after being packed for export? If so, where are they staged and for how long?

Port of Export:

- When was the last time the United States Coast Guard, International Port Security Program (IPSP) visited the port facilities?
- Has the foreign port been certified that it is adequately following the International Ship and Port Facility Security (ISPS) Code?

Mode of international transport and number of legs:

- Is your cargo exported via air, ocean, land, or multiple modes?
- Once shipped, what route(s) do the goods take?
- If shipped ocean/air, is it transshipped to another port, or does it sail/fly directly to a U.S. Port?
- If transiting another port, is your freight remaining onboard (FROB) while other freight is loaded or discharged?
- If offloaded, is it loaded directly onto another vessel/plane?
- If not, does it remain in the same IIT/container, or is it deconsolidated and stuffed into another IIT?
- If offloaded, what is the average time in port before being laden on a vessel/plane bound for the United States?
- If awaiting another vessel/plane, where are the goods stored before it is loaded?

Trading companies/buying agents:

- Do you import from any trading companies or via a buying agent?
- If so, do you know where the goods are actually manufactured/packed for export?
- Are they consolidated?
- If your company purchases goods from a trading company/agent, you must ensure there is transparency in the supply chain and that security measures are in place at the point of origin (factory/warehouse) and throughout all nodes in that chain.

Attachment D, Sample of Simplified Cargo Flow

Supply Chain Flow from XYZ (Supplier) to ABC (Importer)

*Note: **XYZ** only ships full containers to **ABC**; there are no consolidation warehouses, etc.*

1. When ***XYZ*** has produced enough product to fill a container, it calls ocean carrier Z, and referencing ABC 's contract number with **ocean carrier Z**, requests a container.

2. When ***ocean carrier Z*** has a container available, it notifies **XYZ**.

3. **XYZ** contacts **truck carrier W** and asks them to bring the empty container from **ocean carrier Z**'s storage yard near the port to **XYZ**'s plant. The distance from truck carrier W's depot to **ocean Carrier Z'**s storage yard is approximately 1.5 km, and is about a 30 minute drive.

4. The driver from **truck carrier W** picks up the empty container from **ocean carrier Z'**s storage yard, hauls it to **XYZ**'s facility, drops it off, and departs. The distance from **ocean carrier Z**'s container storage yard to **XYZ'**s facility is approximately 35 km, and is about a 2-hour drive.

5. **XYZ** then contacts the foreign government's Treasury Office to schedule an official to come and witness the loading of the container.

6. **XYZ** also contacts **truck carrier W** and schedules a driver to haul the sealed container to ocean **carrier Z'**s yard at the port on the same day.

7. Occasionally, it is necessary to hold the empty container overnight, and stuff it on the following day. In such cases, the container is locked with a padlock.

8. On the day the container is scheduled to be loaded, the Treasury official and **truck carrier W**'s driver arrive at **XYZ**'s facility and witness the container being stuffed and sealed. This procedure typically takes about an hour.

9. **XYZ** prepares an invoice, packing list, bill of lading, and any other documents required for the export shipment, and forwards them to the various parties.

10. The **truck carrier W** transports the sealed container on the specified route, (approximately 35 km for about 2 hours 30 minutes), to **ocean carrier Z'**s receiving dock at the port.

11. The sealed container may wait at **ocean carrier Z'** yard for up to seven days, depending on the schedule of available transport vessels.

12. **Ocean carrier Z** has no direct shipping routes from India to the United States, so the container is loaded onto a ship to country X, where it is off-loaded and staged (one or two days). It is loaded onto a vessel and shipped to the United States.

13. Upon arrival at the U.S. port (city), **ocean carrier Z** arranges for **highway carrier T** to pick up the container to deliver it to **ABC** after the cargo is unloaded.

14. **Highway carrier T** delivers the sealed container to **ABC**, which takes about 2 hours.

Attachment E, Sample of Mapping Cargo Flow and Partners

Step 1 (Sample) Map Cargo Flow, Identify Partners and Processes

Notes: Ensure partners map out all variations of a supply chain: for example, Full Container Load (FCL) vs. Less than Container Load (LCL); from one factory to various ports of export; from one factory using different modes of transportation (air vs. sea); Any other potential variations that would alter the movement of cargo or the individuals involved in the process.
Always remember: **"freight at rest is freight at risk."**

Sub-contracting increases risk within a supply chain, particularly where security requirements have not been conveyed or verified. *Items below in "red" font and an *, indicate a potentially high risk situation*.

Business partner	Role/Process	Cargo movement, if applicable	Known details about provider	Days cargo "at rest" this stage	Trans-port mode	If handles cargo, who selects the provider?
XYZ Manufacturer	Production, Packing, Document Preparation	Point of Departure	Location: City 123, Country Origin; Years doing business with - 22; family owned and operated	0	NA	NA
Export Broker/ FF	Prepares Documentation for Export	N/A	Unknown *	NA	NA	NA
Foreign Inland Carrier ABC	Inland Transportation	Picks up cargo from factory and consolidator EFG	Location: City 123, Country Origin; Contracted by factory - in business 15 years; parent company, CTPAT in USA	0	Truck	Factory
Consolidator LMNOP	Unloading, Storage, Load-ing	Unloads cargo from inland truck carrier, stores LCL, loads with other customers' cargo	Location City 123, Country Origin; Contracted by fac-tory - in business 2 years	2	NA	Factory
Inland Carrier JKL	Inland Transpor-tation	Picks up cargo from consolidator and transports to Port of Export	Location: City 123, Country Origin; Contracted by consolidator's main carrier (123) ; in business 10 years	0	Truck	Consolidator's contracted carrier*

Business partner	Role/Process	Cargo movement, if applicable	Known details about provider	Days cargo "at rest" this stage	Trans-port mode	If handles cargo, who selects the provider?
Port Terminal - Origin	Storage	Receives and stores container in container yard until ready to go on vessel	Location: City 456, Country Origin; operated by government body; MTSA/ISPS compliant	4	NA	Left blank
Sea Carrier	Transportation	Transports cargo from port of lading	Location: City 456; Country Origin; Contracted by importer; in business 20 years; Parent company; CTPAT in USA	3	Vessel	Importer
Port Terminal - Transit Country	Storage	Receives offloaded container at country of transshipment	Location: City 183, **Transit Country; unknown; Unknown MTSA/ ISPS compliant***	**10***	**NA***	Sea Carrier
Sea Carrier	Transportation	Transports cargo from country of transshipment	**Location: City, New Country; unknown**	10	Vessel	Consolidator
Port Terminal - USA	Storage	Unloads cargo from sea carrier's vessel and stores until domestic transport picks up	Location: City 42, USA ; MTSA/ISPS compliant	1	NA	U.S. Consolidator
Domestic Drayage Carrier Picks up	Transportation	Picks up cargo from terminal	**Unknown***	0	Truck	U.S. Consolidator
Consolidator/ Deconsolidator	Unloading, Storage, Loading	Receives LCL cargo, consolidates, ships to destination	Location: City 42, USA - Cross dock facility	1	NA	Importer
Long Haul Carrier	Transportation	Transports cargo to distribution center	Location: City 50, USA -	0	Truck	U.S. Consolidator
U.S. Distribution Center/ Consignee	Unloading	Receives cargo	Location: City 53, USA	0	NA	Importer

Attachment E, Example of Cargo Flow and Partners, Ocean Cargo LCL

Attachment F, RESOURCE LIST*

The National Counterterrorism Center:
www.nctc.gov/

U.S. Department of State - Terrorist Threats/Country Information:
www.state.gov/j/ct/rls/crt/

State Dept. Overseas Security Advisory Council:
www.osac.gov

Department of Commerce Denied Person/Parties' List:
www.bis.doc.gov/dpl/default.shtm

Container Security Initiative (CSI) Ports:
www.dhs.gov/container-security-initiative-ports

7 Signs of Terrorism:
www.youtube.com/watch?v=R8atNS7U5QgI

Information Technology Security Publications:
www.us-cert.gov/security-publications

International Air Transport Association (IATA):
www.iata.org/whatwedo/security/Pages/index.aspx

CIA World Fact Book:
https://www.cia.gov/the-world-factbook

FBI Infrastructure Security:
www.infragard.net

International Chamber of Commerce (ICC) Commercial Crime Services:
www.icc-ccs.org/ www.icc-ccs.org/piracy-reporting-centre

Combined Maritime Forces Counter-Piracy:
www.combinedmaritimeforces.com/ctf-151-counter-piracy/

The Center for International Maritime Security:
www.cimsec.org/

**Note: CTPAT partners should also consult with local law enforcement when conducting threat assessments. In addition, there are many private for profit organizations who offer security risk assessment services.*

This list is not all inclusive and is not meant to be an endorsement of any organization or service.

Attachment G, Sample Threat Assessment

Step 2: Sample Threat Assessment			
Risk Rating: 1 - Low Risk—No recent activity/intelligence/information 2 - Medium Risk—No recent incidents/some intelligence/information on possible activity 3 - High Risk—Recent incidents and intelligence/information Note: For CTPAT Purposes, a 3 for any of the threat risk factors below would result in a high-risk rating for the supply chain.			
Date of Assessment:	**Assessment Conducted by:** *(Provide name of employee who conducted the assessment)*		
List Business Partners: *(List what partners the assessment pertains to, unless too many to list, e.g., numerous employees)*			
Location: Country XYZ			
Region: Region JK	**Overall Threat Rating High**		
Threat Risk Factor	**Risk Rating**	**Activity**	**Source**
Terrorism (Political, Bio, Agro, Cyber)	3	2019, 2020—Recent domestic bombings and violence against U.S. based interests	Name of news publication, government site, open source information, Intel service, etc.
Contraband Smuggling	3	2019, to present— location known for narcotics exports and weapons smuggling	Name of news publication, government site, open-source information, Intel service, etc.
Human Smuggling	1	2000 to 2018— numerous incidents of human smuggling; none since 2018	Name of news publication, government site, open-source information, Intel service, etc.
Organized Crime	1	1998 to 2017—Drug cartels operating throughout country/ region	Name of news publication, government site, open-source information, Intel service, etc.
Conditions within a country which may foster any of the aforementioned threats (e.g. poverty, social unrest, political instability)	2	Demographics—35% population lives in poverty; a few social movements underway with anti-western sentiments	Name of news publication, government site, open-source information, Intel service, etc.
Other: Theft, Pilferage, Hijacking, Piracy, or Intellectual Property Rights (IPR)	2	2018—Incidents of piracy along shipping route; none reported since late 2018	Name of news publication, government site, open-source information, Intel service, etc.
Overall Threat Risk Rating = 3			

Attachment G, Sample Threat Assessment

Attachment H, Sample Cargo Flow and Risk Rating, Manufacturer

Supply chain for 123 Dress Manufacturer					
Location: City J, Country IJK		**Overall Threat Risk: Medium for foreign portion**			
Partner	**Process/Role**	**Cargo Movement/Flow**	**Details About Partner**	**Risk Rating**	**Comments**
123 Dress Manufacturer	Production and packing of finished goods for export.	Point of origin	Medium sized facility, 200 employees, onsite dormitories; ships FCLs only; 24-7 security guards, CCTV *	(2) Medium	No CTPAT validations, but 3rd party audit in 2018.*
XYZ Trucking company	Truck carrier	Transports empty containers to ABC. Transports loaded containers to warehouse/freight forwarder, about a 2 hour drive each way.	Local small trucking company contracted by ABC.	(3) High	2020, Country IJK ranks third in region A for cargo thefts. Hijackings occur; gangs also stop trucks in some areas to extort them to pay "fees" to pass through their territory.
ABC warehouse & freight forwarder	Stores freight and prepares shipping and export documents	Finished goods stored while awaiting shipment to the U.S. ABC arranges for the ocean shipment.	Located close to the POE. Has security guards and CCTV coverage.	(3) High	Access controls are often not enforced in Region A, and corruption is a problem with low wages being prevalent.
DEF Delivery Services	Truck carrier	Transports loaded containers to port terminal (about a 10 minute drive.)	Owned by ABC. Close proximity to POE.	(3) Medium	
Port of TP	Port of Export	Containers are loaded on vessels for export to the U.S.	State owned, 3 terminals, ISPS status unknown. Guards 24-7 and CCTV coverage.	(2) Medium	ABC has visited and viewed security measures.
U.S. portion of the supply chain					
Port of Long Beach	Port of Entry	Containers unloaded	POE	(1) Low	
PW Carrier	Drayage Carrier	Transports containers to MM distribution center about a 45 minute drive.	Local medium sized carrier, drayage only.	(1) Low	Carrier is not eligible for CTPAT, but has contractually agreed to follow CTPAT criteria.
MM distribution center	Unloads containers. Warehouse storage of goods.	Receives the cargo from PW.	Has CCTV coverage and electronic access controls. Access to dock area restricted.	(1) Low	Warehouse is not eligible for CTPAT. Visited as part of a validation for another company in 2018.

**See company survey, last updated September 2019*

Attachment H, Sample Cargo Flow and Risk Rating, Manufacturer

Attachment I, Sample Cargo Flow and Risk Rating, Highway Carrier

ABC Transporte, Supply Chain for Client XYZ Factory			**Threats**		
Location: City K, Country MNO to City S		**Overall Threat Risk: High**	**Smuggling of narcotics and people are ongoing threats.**		
Partner	**Process/Role**	**Cargo Movement/Flow**	**Details About Partner**	**Risk Rating**	**Comments**
XYZ Manufacturer	Production and packing of finished goods for export. U.S. Export documentation preparation	Point of origin	Medium sized facility, 150 employees; makes medical devices; ships FTLs only; Security guards, CCTV. Transporting FTLs for the company for 5 years.	(1) Low	Member of CTPAT; Verified via SVI page.
Export Broker	Prepares foreign Shipping Document	Documentation	Small company that has worked with XYZ for 15 years. Driver must stop in transit to pick up document.	(3) High	Close proximity to Port of Entry.
Border POE	Port of Export/Entry	Border crossing	Government run facilities	(1) Low	
U.S. portion of the supply chain					
EB Distribution Center	Warehouse, unloads cargo	Receives the cargo	Large 3rd party commercial operation	(1) Low	

Cargo flow for ABC Transporte's Client XYZ Manufacturer:

Receives a call to pick up cargo at XYZ:

1. A tractor with an empty trailer is dispatched to the facility, about a 10-minute drive.
2. The driver watches the loading and sealing of the trailer.
3. The driver verifies the seal number against the documents.
4. The driver transports the trailer to the Broker (about a 5-minute drive) to pick up the Pedimento.
5. The driver transports the cargo to the U.S. border crossing, about a 4-minute drive.
6. After crossing into the U.S., the driver proceeds to the U.S. distribution center, about a 40-minute drive.
7. The driver watches the unloading of the trailer.
8. The driver returns the empty trailer to the company yard from abroad, which is located with the dispatch office.

Attachment J, Sample Simplified Risk Analysis for Broker

Threat	Vulnerability	Geographic import region	Risk Rating	Mitigation methods	Source of information/EOI	Action plan item
Attempting to enter terrorist or terrorist weapons into the U.S. Contraband Smuggling (such as weapons, drugs, cash, or IPR) Human Smuggling	Customers New Customers (new business) Personal Shipments/ onetime shipments	Country A Country B Country C	Medium High High	Procedures for Screening Business Partners CTPAT/MRA member* Outreach to customers to join the CTPAT program* Request cargo security measures Provide training materials/outreach for threat awareness Compliance audits of contractors	Client screening protocols Security questionnaire Onsite audit protocols Client outreach materials	(if you don't do something from the mitigation methods, example for an action item)
Contamination of Food Supply—bioterrorism	Produce Imports Seafood Imports	Country A	Low	Send educational materials to clients for threat awareness and methods of prevention	Client outreach materials	
Identity theft of clients by parties attempting to enter illegal/ contraband or terrorist weapons into the United States.	Employees (Internal Conspiracies) Customers' or other Business Partners' security being compromised	Country B	Medium	Ensure Importers track all imports via ACE. Measures to prevent employees from stealing information Send educational materials to clients for threat awareness and methods of prevention	Client outreach materials Access/IT controls Audit protocols	
Theft of sensitive information via compromised IT system	IT system	NA	High	Cybersecurity MSC and other methods to protect against intrusion	IT protocols	

**Is a mitigation method for all listed vulnerabilities*

Attachment J, Sample Simplified Risk Analysis for Broker

Attachment K, Definition of Terms

Table of Contents

Instruments of International Traffic (IIT), for CTPAT purposes: 30

International1 Supply Chain Security, for CTPAT purposes: 30

International Supply Chain Security Risk Assessment: 30

Key Cargo Criteria: 30

Loading/Unloading: 30

Mapping Cargo Flow/Involved Parties: 30

Packing: 32

Purcurement/Purchasing: 32

Production: 32

Risk: 32

Risk Rating: 32

Staging/Storing: 32

Supply Chain Security Action Plan: 32

Top Tier Criteria (TTC): 32

Transportation: 32

The definition of terms below is intended as a guide for the risk assessment process and when examining the roles of parties involved in the international supply chain.

Instruments of International Traffic (IIT), for CTPAT purposes:
Containers, trailers, 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.

International[1] Supply Chain Security, for CTPAT purposes:
From the cargo's point of origin (factory/farm) until its arrival and first point of distribution in the United States, ensure the following seven processes are secure:

- Procurement/Purchasing;
- Production;
- Packing;
- Staging/Storing;
- Loading/Unloading;
- Transportation; and
- Document Preparation.

International Supply Chain Security Risk Assessment:
Process of identifying the security threats and vulnerabilities throughout the international supply chain and prescribing corrective actions with follow-up procedures to ensure weaknesses have been mitigated.

Key Cargo Criteria:
The criteria that is of utmost importance is the one that is aimed at preventing cargo/conveyance/instruments of international traffic (IIT) tampering. This includes sealing requirements, secure storage, inspections, and adequate monitoring and tracking of conveyances and IIT as well as ensuring cargo staged overnight is secure.

Loading/Unloading:
Placing cargo in/on or taking cargo out/off an IIT, including containers, trailers, vessels, planes etc.

Footnote 1: *Throughout the 5-Step Risk Assessment guide, it references the traditional supply chain model of imports coming into the United States. However, for U.S. exporters, it would need to reverse that model to a supply chain flowing out of the United States.*

Mapping Cargo Flow/Involved Parties:
Method of identifying all parties involved and their prospective roles in the seven supply chain processes[2] throughout the international supply chain of cargo destined for the United States. All partners involved both directly and indirectly in exportation/movement of the goods from the point of origin to the importer's distribution center must be included. Some examples of parties involved in the international flow of cargo include, but are not limited to, the following:

- Factories;
- Farms/fisheries;
- Export packing facilities;
- Buying/selling agents;
- Suppliers (excluding raw materials[3] for foreign factories);
- Trading companies;
- Customs broker (import/export);
- Foreign Customs agents;
- Third party logistics providers (3PLs)/freight forwarders;
- Non-vessel operated common carriers (NVOCCs);
- Warehouse/consolidation/deconsolidation facilities;
- Rail depots;
- IIT (trailer/container) yards;
- Shipyards;
- Inland (domestic/drayage) truck/rail carriers;
- Security stop to verify seal;
- Transfer facility (from long haul carrier to drayage or intermodal);
- Feeder vessels;
- International air/rail/sea/truck carriers;
- Handling agents (load/unloads vessels/aircraft);
- Ports/terminal operators (Port of Export, transshipment, Port of Entry); or
- U.S. third party distribution center/warehouse.

Simply put, it is a diagram (or sequential list) of the journey the goods take on the way to the United States that includes the physical movement, the location of the goods, and the chain of custody throughout the CTPAT defined supply chain.

Footnote 2: *The seven supply chain processes to be secured are procurement/purchasing, production, packing, staging/storing, loading/unloading, and document preparation.*

Footnote 3: *Usually, raw materials are excluded from the risk assessment process; unless the raw materials themselves could be dangerous, for example, scrap metal from certain countries may be at risk for Cobalt 60 contamination. Another reason to examine raw materials is if they are at risk for employing forced labor.*

Packing:
Encompasses both packing the goods for export into non-reusable containers and reusable instruments of international traffic (IIT). It includes, but is not limited to, placing goods in/on pallets, cartons, cardboard boxes, crates, bins, or other specialized containers. It also entails bundling, wrapping, shrink-wrapping, and other types of packaging.

Procurement/Purchasing:
Ordering products or services from business partners in the international supply chain. Raw materials that go into making the exported products are usually excluded from this process. This normally pertains to finished cargo/raw material that will be exported to the United States. Services include indirect procurement methods for goods shipped to the United States such as buying agents and trading companies.

Production:
Making, growing/harvesting, or assembling products to be exported to the United States.

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 Rating:
Assigning numerical/other values to threats and vulnerabilities identified during a supply chain security risk assessment (e.g., 1-Low, 2-Medium, and 3-High).

Staging/Storing:
Placing products and/or IITs at a location of "rest" prior to or during movement to the United States. This includes any warehousing/consolidation/deconsolidation of goods and/or facilities where goods wait to be loaded onto another transit mode such as a rail depot or shipyard in the country of origin or other countries the goods may transit through on the way to the United States.

Supply Chain Security Action Plan:
Identifies security weaknesses found during the risk assessment process for a business partner. The plan assigns responsibility for corrective actions/mitigation strategies (internal and external), establishes deadlines/timeframes, documents evidence of actions taken, outlines processes used to verify actions have been taken, and delineates the final outcome.

Top Tier Criteria (TTC):
Top Tier Criteria (TTC) are the criteria that have historically proven to be the most important in preventing a supply chain breach. Since the international portion of the supply chain is at higher risk, the business partner criteria is extremely important. Additionally, the transportation leg is the highest risk area, and supply chain breaches often involve internal conspiracies with employees as key players. Thus, the TTC usually consists of the Key Cargo Criteria, Personnel (for screening employees), and Business Partners' criteria.

TTC may vary for an individual supply chain based on the supply chain's risk assessment. Factors that affect the TTC for a facility are its geographic location, the configuration of the supply chain, and the number and relationship of the supply chain partners involved. Thus, additional criteria may be elevated to top tier level or reduced as appropriate. For example, due to the high risk in a particular country, Physical Security is often elevated to a top tier level in those supply chains.

Transportation:
Movement of cargo throughout the international supply chain. Transporting the goods for export to the United States includes any domestic legs of the goods' journey in the country of origin to the Port of Export, from the Port of Export to any countries that the goods may transit through, to the U.S. Port of Entry, and to the U.S. domestic distribution center.

Attachment L, General Vulnerabilities for Non-Importers

General Vulnerabilities:

- Pseudo/phony customers—criminals trying to pass as legitimate customers to facilitate smuggling or money laundering;
- Indirect customers (for example, subcontracted carriers may know little about loads being transported);
- Many entities own equipment/conveyances/instruments of international traffic (IIT) that they have little control over (for example, sea containers transit the world, too many parties involved in their use, storage, and transport);
- Lacking control over other partners in the supply chain;
- Internal conspiracies (may involve multiple partners);
- Stowaways;
- Multi-day transit times make it more difficult to track and monitor conveyances;
- Compromised conveyances utilized to smuggle contraband/people;
- The commodity imported may be susceptible to specific threats (for example, produce shipments from Mexico, which have been targeted by drug smugglers, or could be used as a bioweapon if contaminated with toxins);
- Transporting hazardous/dangerous cargo that could be weaponized (for example, oil tankers could be modified for use as an explosive device in a port, much like planes were used during 9-11); or
- Inadequate training of personnel could prevent the discovery of a security breach within your supply chain.

Possible Vulnerabilities for Brokers and Consolidators:

- Personal shipments;
- One-time shipments (walk ins);
- Non-Resident Importer;
- Using the broker's Importer of Record (IOR) for a client's shipment;
- Allowing another broker to use your filing code;
- Identity theft of a customer (by another business partner or from an employee);
- Manipulation of shipping documents (via unauthorized access of IT system by an employee/unauthorized entity);
- *Using agents (not controlled by your company) to move cargo;
- Third party Power of Attorneys (freight forwarders); or
- Physically handles cargo.

Possible Vulnerabilities for Sea Carriers and Marine Terminals:

- To many employees with access to sensitive areas;
- Access controls that are not enforced;
- Employees that do not have a valid Transportation Worker Identification Credential (TWIC) ID (or foreign port ID);
- Tampered seals on stored containers are difficult to identify without the proper training; use of the VVTT is an effective method of identifying seals that have been tampered with;
- Improper stowage of hazardous goods;
- Contraband may be smuggled on or inside of the structure of the vessel.

- Inadvertently shipping stolen cargo from the United States to another country;
- Inadvertently shipping cargo that violates intellectual property rights (IPR) to the United States; or,
- Piracy of vessels.

Possible Vulnerabilities for Air Carriers:
- Contraband may be smuggled in the aircraft itself, (structure, seats, compartments);
- Contraband may be smuggled in food carts or luggage;
- Service personnel (cleaning and catering) and crew have access to the aircraft without supervision of authorities;
- Controlling entry into the aircraft via the ramp and passenger door;
- Cargo inspections including that of Known Shippers (self-inspections); or
- Hauling palletized goods; have pallets been examined or x-rayed for anomalies?

Possible Vulnerabilities for Rail Carriers:
- No gates, enclosed perimeters, or cameras monitoring yards;
- Difficult to control access to facilities and equipment while in transit or staged;
- Multiple scheduled/unscheduled stops while in transit;
- Passes through areas where trains must travel slowly;
- Easy to stop/derail a train by damaging railroad ties or placing objects on rails; an easy method to stop trains is a red flag on the track—an industry rule signaling a required stop;
- Using older generation rail cars that are easier to manipulate;
- Not sealing at exact location of loading;
- Not affixing seals at top portion of containers—for double stacked intermodals;
- Staging rail cars (empty or loaded) outside yards for long periods of time; or
- No record of automatic equipment identification (AEI) data for a particular rail car (due to outdated or inoperable equipment).

Possible Vulnerabilities for U.S. Exporters:
- Inadvertently having shipments of dual use or licensed goods diverted to forbidden destinations (countries/persons); or
- Cargo breaches to smuggle weapons or money to a criminal element.

Possible Vulnerabilities for Highway Carriers:
- May have many different types of customers with numerous requirements; this may confuse dispatch, the drivers and those tracking the movement of cargo;
- Hauling pre-loaded trailers/containers (drop and pull/pick);
- Hauling third party owned trailers;
- Hauling various conveyance types: trailers, rail/ocean containers, flatbeds, tankers, reefers; this can be confusing when attempting to identify areas of concealment by identifying items that might be out of place such as extra rivets, a floor that is thicker than usual, or a ceiling that appears lower than it should be;
- Long haul multi-day trips;
- Hauling loads that have been stored waiting to cross the border;
- Hauling less than full loads (LTLs) or empties can leave lots of space for contraband to be loaded;
- Using subcontracted carriers/owner operators that are unfamiliar with CTPAT security criteria;
- Hauling goods as a subcontracted carrier for another carrier (or via truck brokers); or
- Relying too much on GPS; Management is not conducting accuracy checks by occasionally escorting conveyances.

Attachment M
Land Border Highway Carrier General Cargo Assessment Worksheet

Customer	CTPAT Yes/ No	Type of convey- ance /IIT hauled	Who owns convey- ance/ IIT	How many hauled per week/ month	Live load versus loaded	LTL FTL Empty	Distance hauled to border	Crosses border Yes/No	Where delivered	Driver's FAST status	Indirect load/ con- tracted carrier

Attachment N, Sample Action Plan

Step 4: Sample Risk Assessment Action Plan and Follow-Up									
Supply Chain Partner Name: Factory XYZ									
Site/Location:									
Point Of Contact Name:			Phone Number:			E-Mail			
Vulner-abiliiity	(if appli-cable) CTPAT Criteria	Corrective Action(s) Requiring/ Mitigation Strategy	Company/ POC to Implement	Progress Review Date	Corrective Action Deadline	Evidence Action Taken	Verified by and Date	Outcome	Comments

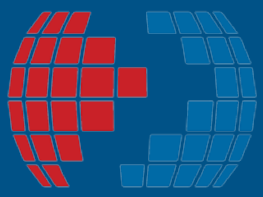
Attachment O, Documenting The Risk Assessment Process (Policy & Procedures)

A company's documented risk assessment process (i.e., policies and procedures) should contain, at a minimum, the following information:

1. Date risk assessment process established/revised (as applicable);
2. Identify personnel responsible for keeping the process up to date, including back-up persons;
3. What will trigger a risk assessment/update outside of a normally scheduled one (e.g., new supplier or service provider overseas);
4. List how often risk assessments must be conducted (e.g., as circumstances dictate or at a minimum annually for most CTPAT partners);
5. Frequency of review/updates of processes/procedures (e.g., annually, bi-annually, as needed, etc.) for the risk assessment policy;
6. Describe how threat assessments of the international supply chain are conducted (e.g., sources used to determine threats);
7. Describe how vulnerability assessments on the international supply chain are conducted (e.g., send surveys, site visits, CTPAT status, and/or participation in a foreign supply chain security program that has signed a Mutual Recognition Arrangement (MRA) with the United States);
8. Describe how follow-up is conducted on action items (e.g., site visits may be required in some cases, for others, documentation/photographs may be submitted);
9. Procedure for training key individuals who are responsible for the processes; and
10. Management oversight and accountability for ensuring the process is carried out consistently and effectively.

Notes

Notes



CTPAT™

YOUR SUPPLY CHAIN'S STRONGEST LINK.



U.S. Customs and Border Protection

Publication No. 1687-0222