C-TPAT

Customs-Trade
Partnership Against Terrorism

C-TPAT's Five Step Risk Assessment

U.S. Customs and
Border Protection

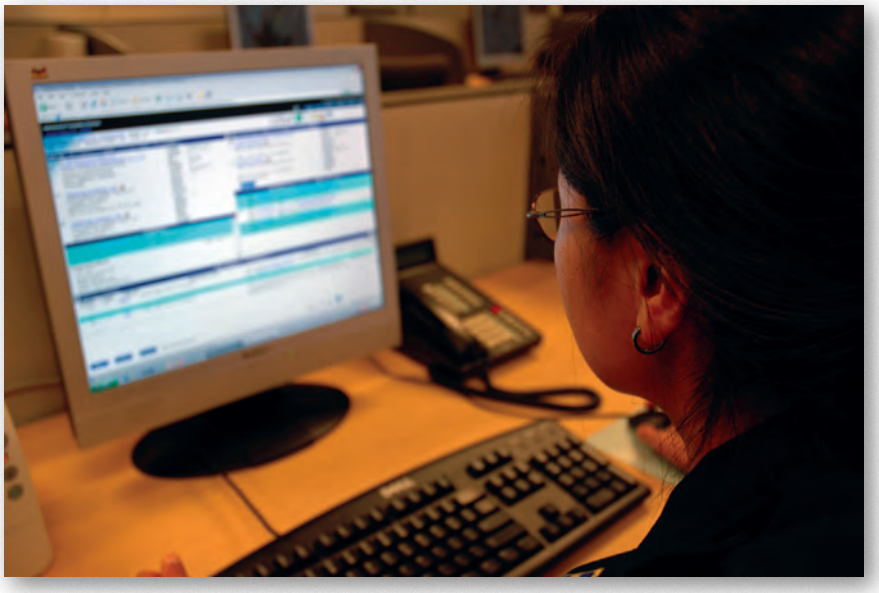
U.S. CUSTOMS AND BORDER PROTECTION

C-TPAT's Five Step Risk Assessment

Table of Contents


Risk Assessment
Severe
High
Significant
Moderate
Low
Very Low

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to strengthen international supply chains and improve United States border security; in exchange, CBP affords C-TPAT Partners certain benefits, including reduced examination rates and access to the Free and Secure Trade (FAST) lanes.



Launched in November 2001 with seven major importers as a direct result of the tragic events of September 11, 2001, the program now includes more than 10,700 Partner companies, and covers the gamut of the trade community to include importers; exporters; border-crossing highway carriers; rail, air, and sea carriers; licensed U.S. Customs brokers; U.S. marine port authority/ terminal operators; U.S. freight consolidators; Mexican and Canadian manufacturers; and Mexican long-haul highway carriers. One vitally important aspect of the minimum security criteria Partners must address to maintain the security of their shipments is a documented risk assessment process.

As a voluntary public-private sector partnership program, C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the principal stakeholders of the international supply chain. Those companies that become C-TPAT Partners are expected to meet and maintain the security standards of the program. Part of that criteria is the requirement for Partners to conduct and document for C-TPAT's review a risk assessment of their international supply chains. The risk assessment process is critically important as it allows Partners to truly understand their supply chains, where the vulnerabilities lie within those supply chains, and determine what to do in order to mitigate any risks identified.

To assist Partners in creating a robust and effective Risk Assessment process, in 2010 C-TPAT published the "5 Step Risk Assessment Guide." Much time and many world events have occurred since then that necessitate an update and enhancement to the initial guide. Not least among these changes are the creation of the C-TPAT Exporter Entity, and the signing of several additional Mutual Recognition Arrangements. C-TPAT has now signed arrangements with the customs agencies of Canada, the European Union, Japan, Jordan, New Zealand, South Korea, Taiwan, and Israel.

Since its inception in 2001, the C-TPAT program has evolved dramatically. During the revalidation process and when conducting an in-depth review of security breaches, it became apparent the process of conducting a security risk assessment was not being adequately performed, often due to a lack of knowledge on the topic. An analysis of validation results for C-TPAT importers in 2013 revealed 22.6% did not have a documented Risk Assessment process that effectively addressed their international supply chains.

The lack of a documented process generated an Action Required in the Partners' validation reports, and those Partners that did not adequately address this Action Required were subsequently removed from the program. Most C-TPAT Partners are conducting a comprehensive domestic risk assessment of their own facilities and processes in the United States; however, many Partners are not assessing the potential threats and vulnerabilities that may exist within their international supply chain from the point of manufacture/packing/stuffing and at each transportation link within the chain, until the cargo reaches the final point of distribution.

As part of the application process to join the C-TPAT program, applicants must be able to provide a documented process of how the company assesses risk. Due to the unique nature of every Partner's business model, the risk assessments described below are only guides, and all companies should establish a process that conforms to the needs of their business model, and not simply adopt a generic, externally provided model. C-TPAT Partners must conduct a risk assessment at least annually in order to remain in the C-TPAT program.

Even small Partners are required to have a documented Risk Assessment Process. In fact, the smaller a Partner is, the easier it is to conduct a Risk Assessment. If, for example, a small highway carrier with an established business model of hauling from a single manufacturer to a single U.S. importer, and not soliciting other clients or using owner-operator truckers, desires to establish a Risk Assessment process, it should take only several hours to conduct and document an effective process. The key is that Partners are expected to implement a proactive approach and mentality to address risk in their supply chains, and not simply shrug the issue off as being out of their control. Partners should keep in mind they have an important resource to assist them in all security-related issues — their assigned C-TPAT Supply Chain Security Specialist (SCSS).

Other concepts to keep in mind include that quantity does not necessarily define risk. An importer who sources 300 shipments a year from a low risk source in a politically stable country with a low risk of terrorism and smuggling should not disregard the risk of importing two shipments per year from a country that has recently had a violent turnover in government, a high corruption index, or has a current history of a low level of security. As a further example, an importer that receives 80% of its shipments from a specific manufacturer may not have a low risk supply chain if the manufacturer selects foreign ground transportation providers based solely on cost. From week to week or shipment to shipment, a manufacturer who frequently changes carriers is much higher risk than a manufacturer who always uses the same foreign trucker who is certified in an Authorized Economic Operator (AEO) program.

In addition to security, there are other issues that may cause delays in the movement of goods through a company's supply chain. Partners willing to take extra steps to reduce unexpected delays for agricultural issues are encouraged to consider expanding their risk assessments beyond security concerns. The use of wood packaging material (WPM) that is improperly treated and/or shows evidence that pests are present may result in substantial delays and additional costs incurred by the importer, i.e., possible liquidated damages, demurrage charges, costs for remedial mitigated action, and potentially even immediate re-exportation of the shipment.

WPM Inspection

WPM is defined as wood or wood products (excluding paper products) used in supporting, protecting, or carrying a commodity. Some examples of WPM include, but are not limited to, bins, cases, cratings, load boards, reels, boxes, containers, drums, pallets, skids, bracing, crates, dunnage, pallet collars, etc.

The supply chains with the highest risk of finding imports with non-compliant WPM are metal, stone, food, and finished wood products, along with machinery, electronics, and plants. All imported shipments arriving into the United States using WPM must be properly treated under the International Standards for Phytosanitary Measures (ISPM 15).

C-TPAT has partnered with CBP's Agriculture Programs and Trade Liaison office to help Partners identify and mitigate the risks posed by the use of WPM in their supply chain(s). If your company imports, exports, or transports goods using WPM, please visit the CBP website for more information and training materials.

As part of a C-TPAT Partner's risk assessment process, C-TPAT Partners are not required to gather specific security-related procedures from business partners who have shared their certified C-TPAT or AEO status with the Partner conducting the risk assessment. The fact C-TPAT or a foreign mutually recognized customs program has validated such a Partner's procedures as meeting the minimum security criteria is intended to save time and effort on both Partners' security verification efforts.

While conducting risk assessments, these C-TPAT or AEO certified Partners should be considered low risk, although this does not mean the risk in the partner's involvement in the supply chain should be disregarded. It does mean the business partner is lower risk than other links in the supply chain, and should be treated accordingly.

"The key to building a successful Risk Assessment Process is to ensure it is unique to your company's business model and practices."

The original "5 Step Risk Assessment" guide in 2010 was written with importers in mind, and since the initial publication many questions and suggestions regarding the other types of Partners in the C-TPAT program have been received. Thus, this guide is broken into chapters for different types of business models, though not necessarily by specific C-TPAT entity classifications. This is because some consolidators might have business models similar to importers, while other consolidators might have models similar to brokers. Third Party Logistics operators may have models similar to highway carriers or to consolidators, and exporters may have models similar to foreign manufacturers.

The key to building a successful Risk Assessment Process is to ensure it is unique to your company's business model and practices. Generic, one-size-fits-all, "cookie cutter," externally inflicted procedures can lead to a false sense of security and an eventual breach of security.

As a lead in to the discussion of risk assessments, we will first define some terminology.

Risk Assessment

A Risk Assessment is analyzing external threats against company procedures to identify where vulnerabilities exist, and what procedures can be implemented or improved to reduce such risk.

This may include ensuring (through process improvement, retraining, working with business partners, etc.) that issues identified through analysis and audits as being vulnerabilities are successfully addressed. This may often be something as simple as clarifying a written policy, automating a process, simplifying a form to ensure more effective use of the form, or requiring the security guard to manually hold and examine identification documents (as opposed to viewing ID as a person walks by). A Risk Assessment consists of several components, including a Threat Assessment, Cargo and Data Flow, Vulnerability Assessment, and audits of security procedures. These steps are further delineated on the following pages.

A Risk Assessment should also include how security procedures would be affected by natural and man-made disasters, to include how backup systems will address these vulnerabilities. Such issues include power outages; weather events such as hurricanes; earthquakes; civil unrest; and terrorist events. Partners seeking to reduce the impact of such disasters should have documented business resumption procedures in place that are periodically tested.

You will note throughout the minimum security criteria that expensive technology is not mandatory, for in the end security relies upon the human component. This is why effective personnel screening and security training are critical issues. As an example, no matter how complicated a computer password is required by an Information Technology policy, if employees practice habits such as writing their passwords on sticky notes or "concealing" them underneath keyboards, security is easily breached.

Threat Assessment

A Threat Assessment is simply identifying threats to a supply chain that exist within a country or region, that are external and outside the control of the Partner, to a Partner's business model. Examples include terrorist activity, drug smuggling, hijacking, corruption levels, and human smuggling. Be aware threats in one state or province of a country may differ from threats in other states and provinces within the same country. Below you can see a snapshot of part of a Threat Assessment developed by a C-TPAT Partner for the region (British Columbia) in which they operate. A full, blank version of this document can be found for your use on the public *CBP.gov* website, under the C-TPAT Resource Library and Job Aids.

Threat Assessment: An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat.
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 C-TPAT purposes, a "3" for any Threat Risk Factor below results in a "High Risk" rating for the supply chain.

Partner: SP Trucking			
Location: British Columbia			
Country/Region: Canada			
Threat Risk Factor	**Risk Rating**	**Activity**	**Source of Information**
Terrorism (Political, Bio, Agro, Cyber)	2	Threats posed by terrorism within Canada, particularly the radicalization of domestic extremists, has been clearly demonstrated through…	Canadian Security Intelligence Service *www.csis.gc.ca*

Threat Assessments should use some type of risk scaling, but this need not be complex. For an importer with dozens of supply chains, a numerical ranking system of 1–10 may be appropriate. For companies with few variances in regions of operations, a limited number of supply chains, and a steady business model, a simple high / medium / low system may be appropriate. The goal is to have a ranked output to determine where your company should focus time, energy, and resources to reduce and mitigate risk.

In the previous Risk Assessment Guide C-TPAT provided numerous internet sites to aid in developing a Threat Assessment. In this edition, internet sites are not being provided as there are literally thousands of useful and informative websites available on this topic. It would thus be presumptive to list only a few of these sites, and considering the extreme variances and complexities within Partners' business models, perhaps counter-effective.

Vulnerability Assessment

A Vulnerability Assessment is identifying weaknesses in a company's security procedures and supply chain that can be used to the advantage of terrorists and other criminals identified in the Threat Assessment. Internal audits and security reviews can be important instruments in identifying vulnerabilities. For example, an internal audit of the company itself (such as an internal audit during the annual security profile review, security questionnaires, and site visits conducted during business partner screening), could go into the overall vulnerability assessment. Corrective actions based on the findings of internal audits and business partner reviews can be implemented as part of the Action Plan. This is how the various actions taken by C-TPAT Partners to address program requirements all interact and overlap to strengthen security overall.

C-TPAT Partners are required to determine and assess the level of risk business partners bring into the supply chain. This is a requirement under the business partner screening section of the minimum security criteria, and information developed as part of that process should be included in determining risk in the appropriate supply chain. Typically, business partners should be analyzed against the appropriate minimum security criteria. For example, the highway carrier minimum security criteria should be used as a tool to assess the practices of, and risk level of, foreign and domestic highway carriers, even if those carriers do not physically cross a border. Similarly, foreign freight forwarders and brokers should be analyzed using the consolidator and/or broker minimum security criteria.

Assigning High Risk Targets

Consider on a personal basis:

You have recently purchased a new vehicle. The vehicle appears as number five on the most frequently stolen vehicle list in the United States for the past two years. This is your Threat Assessment, the external threat to your vehicle over which you have no control. You may need to further research this issue on-line, or by contacting local police departments and insurance companies, to determine if the threat in your area is higher or lower than the national average. Your insurance rate no doubt already includes risk factors of national and local theft rates.

A Vulnerability Assessment is next, which describes where your vehicle is susceptible to theft, and should include issues such as:

- Do you live in an area known for a high vehicle theft rate?
- Do you frequently use street parking at home and at restaurants, or do you lock the vehicle in your garage and only use secure parking lots or valet parking?
- Do you live on an island connected to the mainland via only a single causeway?
- Is it a convertible, with easier access than a traditional hardtop vehicle?

Once these vulnerabilities are identified and documented, you are ready to proceed to the next step, completing an Action Plan that will put into place procedures to reduce or mitigate the threats identified above.

Action Plan

An Action Plan consists of once having identified and documented vulnerabilities, developing and implementing procedures and/or improvements to reduce those vulnerabilities. In severe instances, a company may decide to withdraw from a high risk supply chain. In some instances, additional direct management oversight in daily operations might be deemed adequate to address the risks (e.g., posting an employee who works directly for the importer at a high-risk foreign manufacturer). In others, the

implementation of additional overlapping, interlocking procedures or technology might be deemed to adequately address and mitigate the risk.

Using the personal vehicle example above, once having identified when and/or where your vehicle is most at risk of being stolen, what procedures do you put in place to mitigate the threat of theft? Examples might include installation of a theft alarm; installation of a false theft alarm by placing stickers on windows and a flashing red light on the dashboard; installation of a remote engine shutdown system; use of only manually attended parking lots/garages or valet parking at restaurants; use of a steering wheel locking mechanism; or registering and tagging your vehicle with the local police as not being allowed on the road between midnight and five a.m.

An audit of these procedures might include ensuring family discussions with all family members (i.e., periodic security threat and awareness training, or "company musters") on the reasons for, and necessity of, following these procedures, and that all persons understand the ramifications a "family member" (i.e., employee) might face for not following such procedures (resultant loss of use of the vehicle).

Audit

An audit is a periodic documented review to ensure the procedures the company has in place are being conducted and followed through on, as part of regular, every day procedures, and that records are completed and properly filed. Audits may reveal security deficiencies, but do not replace, rather enhance, a company's Vulnerability Assessment. For a sample Audit procedure incorporating the entirety of the minimum security criteria, see the chapter on Brokers.

Recommending a Risk Assessment Process

In order to assist C-TPAT Partners with conducting a risk assessment of their international supply chain(s) in accordance with the C-TPAT minimum security criteria, a Five Step Risk Assessment Process is recommended.

This reference guide contains some of the basic tools, resources, and examples C-TPAT partners should consider using when conducting a risk assessment of their international supply chain(s). The information contained herein is intended to serve as a guide, and is not "all inclusive" of what should be included in an international supply chain security risk assessment. For various free examples of some of these procedures and the suggested evidence of implementation, please see the Resource Library and Job Aids page on *CBP.gov*.

The Five Step process described below can be used by Partners of all entities to determine what threats exist to their business models, even if a Partner does not physically handle cargo. Those Partners that only handle data are also at risk, for if a terrorist or other criminal seeks access to a cargo shipment, the first thing they require is knowledge of a shipment and the identifying information of the companies involved in the cargo movement.

An example of how the C-TPAT minimum security criteria addresses these issues is under Broker Procedural Security, "Security measures must be in place to ensure the integrity of any data or documents relevant to security of processes, transportation, handling, and storage of cargo in the supply chain."

While many Partners use a numerical rating system to assess risk, an alternative method can be used. It is up to each Partner to determine how risk will be assessed. The threat and vulnerability factors described in this document should be used to determine the level of risk, which should be described

appropriately (e.g., high, medium, or low; acceptable or unacceptable; pass or fail, etc.). A complex rating system may be used, but is not appropriate for all business models.

Partners should be aware that Incoterms have little to do with security assessments for terrorism and criminal activity. Incoterms are primarily directed towards cost, ownership, and insurance purposes. A terrorist willing to explode a device within a U.S. harbor, or a human trafficker impersonating a legitimate shipment through identity theft, cares not for legitimate ownership and insurance claims. The C-TPAT Partners responsible for the importation and exportation of goods across U.S. borders, no matter where the actual transfer of ownership occurs, are ultimately responsible for the security of that shipment, regardless of the Incoterms. The acknowledgment of this fact, and the willingness to be proactive and energetic in addressing supply chain security, is what separates C-TPAT Partners from those who are not Partners. Companies that feel the requirements of the C-TPAT minimum security criteria are too burdensome are not suited for the C-TPAT Program. For exporters particularly, it is critical shipments are protected from threats to U.S. allies to whom shipments are destined. The reputation of the entire U.S. business community rests on exporters being proactive and conscientious of their responsibilities concerning supply chain security. It is thus critical for the survival of all C-TPAT Partners to be aware, and selective of, its business partners.

The Five Step Risk Assessment Process includes:

1. **Mapping Cargo/Data Flow and Control and Identifying Business Partners** (whether directly or indirectly contracted) and how cargo moves throughout the supply chain to include modes of transportation (air, sea, rail, or truck) and nodes (country of origin, transit points).

2. **Conducting a Threat Assessment** focusing on Terrorism, Contraband Smuggling, Human Smuggling, Agricultural and Public Safety Threats, Organized Crime, and conditions in a country/region which may foster such threats, and ranking those threats.

3. **Conducting a Vulnerability Assessment in accordance with the C-TPAT Minimum Security Criteria.** A vulnerability assessment includes identifying what the Partner has that a terrorist or criminal might desire. For brokers this might be data; for importers, manufacturers, and exporters, this might be access to cargo and company information. Then, identifying weaknesses in company procedures that would allow a terrorist or criminal to gain access to these processes, data, or cargo.

4. **Preparing a Written Action Plan to Address Vulnerabilities.** This includes mechanisms to record identified weaknesses, who is responsible for addressing the issues, and due dates. Reporting results to appropriate company officials and employees on completed follow up and changes is also essential.

5. **Documenting the Procedure for How Risk Assessments are Conducted, to Include Reviewing and Revising the Procedure Periodically.** The process itself should be reviewed and updated as needed at least annually, and a Risk Assessment should be conducted — and documented — at least annually, more frequently for highway carriers and high risk supply chains.

It is understood that some C-TPAT Partners have numerous supply chains, which may present a major task when conducting a comprehensive security risk assessment of their international supply chains. Therefore, it is recommended that C-TPAT Partners first identify their "High Risk" supply chains by conducting a threat assessment at the point of origin/region and where the cargo is routed/transshipped, and then conducting

a comprehensive security vulnerability assessment of those supply chains. Subsequently the Partner should address the supply chains identified as medium and then low risk. This is to ensure the assumptions made in identifying risk levels as medium or low are in fact accurate. Companies that seek to elevate their security procedures to a Tier III status would be expected to complete threat, vulnerability, and risk assessments on all partners and supply chains.

Documenting the Risk Assessment Process

The five-step process above is generic in nature to allow its application to all business entities and models. A sample Risk Assessment Procedure, as described in Step Five above, is displayed here. A company's documented risk assessment process (e.g., policies and procedures) should contain, at minimum, the following information:

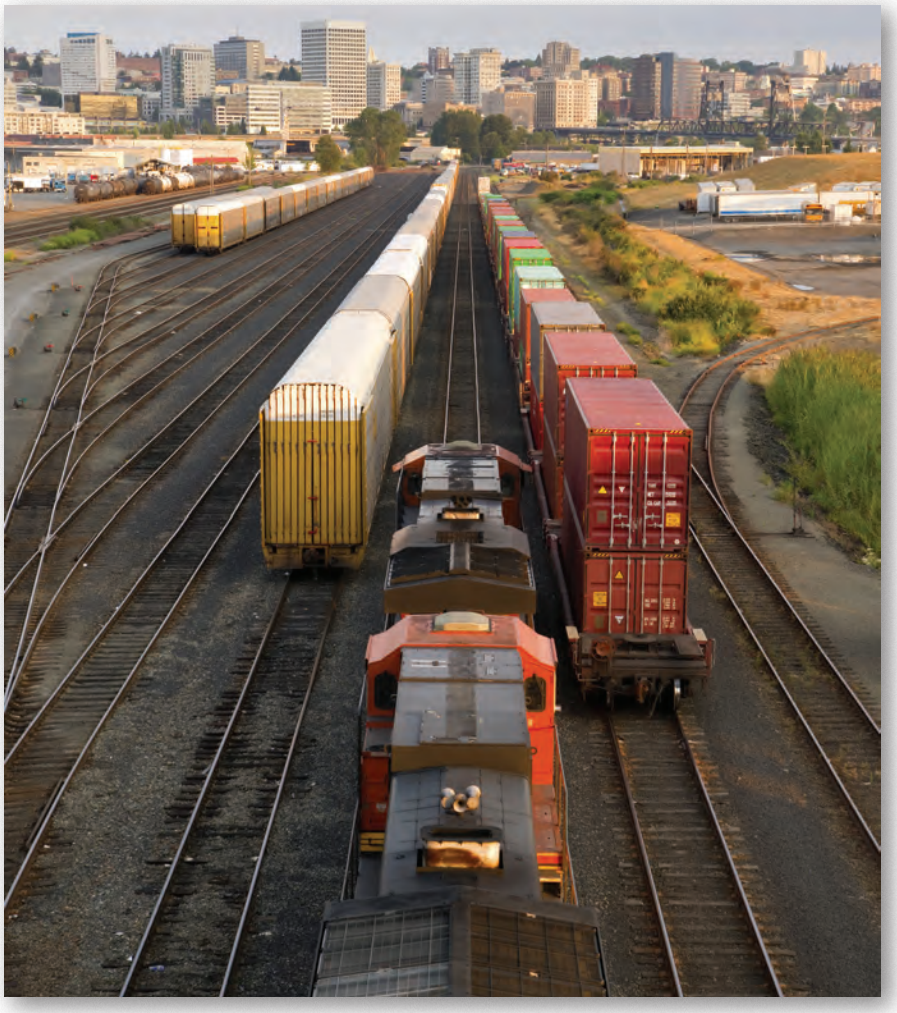
1. Date the Risk Assessment Process was established by the Partner, and latest revision date.
2. Identify company personnel responsible for keeping the process up-to-date, including "back-up" personnel.
3. When or how often a Risk Assessment must be conducted (e.g., annually, quarterly (recommended especially for highway carriers); a new business partner in a supply chain; threat conditions change in a country or region).
4. Required frequency of review and update to the actual Risk Assessment procedure (e.g., annually, quarterly, etc.).
5. How Threat Assessments of international supply chains are to be conducted.
6. How Vulnerability Assessments on the International Supply Chain are to be conducted (e.g., verification of C-TPAT/PIP/AEO Status, site visits by Quality Assurance Managers, analysis of completed security questionnaires).
7. How follow-up is conducted on "action items" (e.g., site visits to address vulnerabilities, termination of contracts).
8. Procedure for training key individuals who are responsible for the Risk Assessment Process, to include regional employees who frequently visit foreign sites for other purposes (e.g., quality assurance managers, sales representatives).
9. Internal management oversight and accountability for ensuring the process is carried out consistently and effectively.

Verifying Radioactive Isotopes Are As Manifested

Chapter One

U.S. CUSTOMS AND BORDER PROTECTION

For importers, the first step in a Risk Assessment is identifying all business partners involved in the knowledge and movement of cargo from point of origin to destination. If an importer cannot identify all steps and business partners in the movement of cargo from origin to destination in the U.S., the importer will not be able to control the security of each step in the supply chain. A sample spreadsheet delineating business partners involved in the movement of cargo from point of manufacture to destination in the U.S. is shown below. Note some supply chains may contain more steps than shown in the example, and some will contain fewer steps.



A modifiable version of the below document for Everything Importers is available on the public *CBP.gov* website, under the C-TPAT Resource Library and Job Aids.

Supply Chain Step	Type of Service Provided	Details About Business Partner	Issues to Consider
Foreign Manufacturer Information	Manufacturer	ABC Manufacturer 183 Jalan Bukit Bintang, Kuala Lumpur, Malaysia. Provides importer approximately 63% of imports.	Not eligible for C-TPAT; country has no AEO program
Highway Carrier (for both FCL and LCL)	Moves cargo from factory to consolidator and port of export	Super Secure Freight, Lebuh Relau, 11360 Bayan Lepas, Kuala Lumpur, Malaysia	Not eligible for C-TPAT; country has no AEO program
Consolidation Facility	Physical location where LCL freight is stuffed into container	FastCon, Building 62, Predak Commercial Zone, Kuala Lumpur, Malaysia	Not eligible, but visited by a C-TPAT team 12/12/2013. Report on file with importer, no Actions Required

Supply Chain Step	Type of Service Provided	Details About Business Partner	Issues to Consider
Highway Carrier	Moves cargo from consolidator to port of export	Reliable Haulers, 168 Jalan Imbi, Kuala Lumpur, Malaysia	Not eligible for C-TPAT; country has no AEO program
Freight Forwarder	Processes paperwork for cargo export, including ISF	Global Freight Coordinators, No 32, 1st Floor, BBandung Lepas, Kuala Lumpur, Malaysia	Not eligible for C-TPAT; country has no AEO program
Port of Export	Stores and handles cargo prior to lading	Pelabuhan Klang, Malaysia	Meets ISPS requirements
Ocean Carrier	Moves cargo from port to port	Excellent Ocean Carriers, 626 Joro Blvd, Pelabuhan Klang, Malaysia	C-TPAT status verified in Portal.
Transhipment Port	Stores and handles cargo in between vessel movements	Kaohsiung, Taiwan	Taiwan AEO Certified, Certificate in Portal Document Exchange
Ocean Carrier	Moves cargo from port to port	Pacific Swells, 5th Floor, No. 2, Chung Cheng 3rd Rd., Xin-Xing District, Kaohsiung City, Taiwan	C-TPAT status verified in Portal.
Ocean Terminal in US	Location of unlading	LA/Long Beach, CA	C-TPAT status verified in Portal.
US Import Broker	Files US import documentation	Paperwork Professionals, 555 Imperial Highway, Suite 816, Los Angeles, CA 90211	C-TPAT status verified in Portal.
Terminal Operator	Handles and stores cargo after unlading	Smith Terminal Facilities, Pier Z, Los Angeles, CA 90809	C-TPAT status verified in Portal.
Domestic Drayage	Trucks cargo from ocean terminal to consolidator or ultimate destination	Porter Transportation, 301 Normandie, Torrance, CA 90518	Not eligible, completed security questionnaire for this year on file

Supply Chain Step	Type of Service Provided	Details About Business Partner	Issues to Consider
Deconsolidator	Cuts seal and unloads container prior to domestic delivery of cargo.	Ochoa Warehousing, 201 Del Amo, Wilmington, CA 90512	Has no bond with CBP, thus not eligible. Security site visit conducted in past three months, results analyzed and on file. Three Actions Required. Uses outsourced day laborers; high risk.
Domestic Drayage	Trucks cargo from ocean terminal to consolidator or ultimate destination	Parsons Parcels and Trucking, 689 Opp St., Los Angeles, CA 90613	Not eligible, completed security questionnaire on file from last month.
Importer	This is our company.	Everything Importers, Address of Receiving Facility	This is our company, see latest Internal Audit on security procedures.

Container Inspections Should Detect Altered Container Frames

Chapter Two

U.S. CUSTOMS AND BORDER PROTECTION

For brokers that do not handle cargo, the primary item they possess and need to safeguard is information. If a terrorist desires to conceal weapons or people in a shipment, the first thing they need is specific knowledge of the shipment. C-TPAT has identified at least two occasions of identity theft targeting brokers, one the theft of identity of a client-importer of the broker to smuggle trademark violation merchandise, and the other an attempt at financial fraud.

For brokers that physically handle cargo, the choice for a risk assessment may be a combination of the broker and consolidator, or even importer, risk assessment processes. When determining how to create a Risk Assessment Process, brokers should consider their business model first. For a broker, steps one through three of the five step process could vary widely depending on the company's business model.

1. **Cargo Mapping**
   - Cargo handler — similar to importer, with addition of broker example
   - Non-cargo handler — use broker example
2. **Vulnerability**
   - Cargo handler — similar to importer, with addition of broker example
   - Non-cargo handler — use broker example
3. **Threat**
   - Cargo handler — similar to importer, with addition of broker example
   - Non-cargo handler — use broker example
4. **Action Plan**
5. **Documented Procedure**

The primary security task for brokers is to control who has access to their data and their clients' data. A full assessment of risks to the data can be identified through an internal audit that includes all aspects of the minimum security criteria, to determine both if procedures are adequate and if security procedures are being followed by employees. By controlling who the broker does business with and who has access to its facilities and data systems, the broker can control who can access its information.

"The primary security task for brokers is to control who has access to their data and their clients' data."

BROKERS

The first step in a risk assessment process for brokers includes an audit of documentation to ensure security procedures are followed on a daily, systemic basis, and that adherence to these standards is adequately documented. Persons conducting audits on various processes should not be those responsible for conducting the work regularly, but someone from another division or assignment. Results of the audits should be documented, to include possible vulnerabilities identified, and suggestions on how to improve and revise procedures.

The process used to conduct the first full risk assessment audit should be documented for future use. The process should be conducted on a scheduled basis, and should include the persons responsible for the completion of the project and those tasked with its parts.

All security-related procedures that have not yet been documented should be documented as part of the first assessment. All procedures and policies should have issuance and revision dates. A broker must consider all aspects of the minimum security criteria.

A more detailed checklist of items that should be reviewed, documented, and followed up on by the broker may be found at the end of this chapter.

Please remember that under the broker minimum security criteria, business partners are broken into two categories: Importer Clients and Service Providers.

An Importer Client is a company that approaches the broker and offers to pay the broker for services rendered to assist in clearing cargo with CBP.

A Service Provider is a business partner selected by the broker to supply services to the broker. Examples of the latter include a domestic drayage company; a de-consolidator; or a freight forwarder.

A visual for possible variations in screening these classes of partners is displayed here:

Importer Clients	Service Providers
C-TPAT status queried, verified, and documented?	C-TPAT status queried, verified, and documented?
Status in foreign program queried, verified, and documented?	Status in foreign program queried, verified, and documented?
Status within ISO 28000 queried, verified, and documented?	Status within ISO 28000 queried, verified, and documented?
Credit checks verified and documented?	Credit checks verified and documented?
Business References verified and documented?	Business References verified and documented?
Original Power of Attorney on file?	Membership in professional organizations verified and documented? (e.g., American Trucking Association)
	Status with U.S. government programs verified and documented? (TSA, IATA, FMC, etc.)
	Written statement (security questionnaire, letter of affirmation, etc.) that non-C-TPAT company is meeting minimum security criteria?
	Site visit for security purposes documented?
	Follow up action plan documented?
	Resolution of action items documented?

At the end of this chapter is a sample listing of some, but not all, of the items a broker might include on its Internal Audit Checklist to ensure employees are conforming to company security procedures. The items are broken down into these general C-TPAT criteria sections:

- **Business Partners**
- **Container and Trailer Security**
- **Procedural Security**
- **Physical Security**
- **Physical Access Controls**
- **Personnel Security**
- **Security Training and Threat Awareness**
- **Information Technology Security**

Audit Checklist

Business Partners

- ☐ Do all C-TPAT Partners show "certified" in the portal? If not, why not?
- ☐ If a previous C-TPAT partner now shows "not certified," have the remaining steps in the business partner screening process been conducted and documented?
- ☐ For all non-C-TPAT business partners, are records up to date with documented evidence of the required additional screening? This might include copies of current PIP/AEO certificates; completed copies of Security Questionnaires; documented reviews and analysis of completed Security Questionnaire; documented site visits; documented follow up on weaknesses; results of background queries, such as Specially Designated National queries, and industry certifications.
- ☐ Have "extra scrutiny triggers" for the screening of business partners been reviewed and updated?
- ☐ Has the company's Preferred Provider List been rescreened and updated?
- ☐ Has the updated list been disseminated to employees and old lists destroyed?
- ☐ Has Outreach/Training on the C-TPAT program been conducted with non-C-TPAT partners?
- ☐ Has the Outreach/Training been documented for each company?
  If yes, in what manner? (On-site, telephonic, web-based, etc.).
- ☐ What topics were covered in the Outreach/Training (e.g., tracking and monitoring, conveyance inspections, seal procedures, notification to our company and customs/law enforcement with discrepancies, access controls, internal conspiracies, challenging strangers)?
- ☐ Have all business partners (both importer clients and service providers) been provided with the broker's contact information for security inquiries?
- ☐ Has the broker's website been updated with C-TPAT information and valid links to *CBP.gov?*
- ☐ What actions were taken to improve processes in this security category?

Procedural

- ☐ **Powers of Attorney —** Does our company have original, current powers of attorney for each active importer client?
  - ☐ If no, what follow up actions are to be taken?
- ☐ **Importer Security Filing —** What score did our company receive on its latest Importer Security Filing Progress Report?
  - ☐ How can this score be improved upon, if necessary?
  - ☐ How and what information was requested from importer clients whose track record requires improvement?
  - ☐ Who was tasked with this improvement?
  - ☐ Have the improvements been completed?
- ☐ **Entry filing —** What is the date of the last audit of entries filed with CBP?
  - ☐ What issues were identified that could be improved upon?
  - ☐ Who was tasked with this improvement?
  - ☐ What steps were taken to complete these improvements?
  - ☐ Have the improvements been completed?
- ☐ **Visitor and Driver Logs —** A manual review of all Visitor and Driver logs must be conducted.
  - ☐ What were the results?
  - ☐ Were all entries complete and legible?
  - ☐ What patterns of concern emerged?
  - ☐ Are there additional items it would make sense to add to the logs?
  - ☐ What actions can be taken to improve the logs?

Below, please find an example of the business processes typically provided by brokers to their client-importers. This Procedural Security breakdown is displayed below to assist brokers in drilling down to determine the level of security procedures in place to protect data.

Supply Chain Step	Type of Service Conducted by Our Company	Process	Risks Identified	Actions Taken to Mitigate Risks
Receipt of entry processing information	Documentation: Receiving in advance of arrival	Brokerage and Import Managers monitor the documentation transfer	Data leakage	Employees of both Departments sign non-disclosure statements. IT Firewall, Anti-virus, Anti-spyware software installed Training computer users on internet threats, to include phishing emails, and how to identify and report suspicious IT activity
Verification of import documents	Verification of Commercial Invoice information and other relevant import data	Brokerage Manager monitors the documentation verification	Overlooking inadequate, or not recognizing tampered documentation	Training appropriate employees on recognizing suspicious shipment and document indicators. Regular Audits and corrective actions
Obtaining and validating Power of Attorney (POA)	Having valid Power of Attorney	Brokerage Manager monitors the POA validation	Mistaken validation	Regular sampling and checking of validated POAs
Verification of description for proper classification	Verification of description for correct classification of imported goods	Brokerage Manager monitors the verification and classification	Misclassification, especially of suspicious goods	Training appropriate employees on recognizing suspicious shipment and document indicators Regular sampling and checking of Schedule B numbers against product descriptions
Contact CBP Website	Perform Bond Query	Brokerage Manager monitors the Bond Query process	Phishing through company internet access and email	IT Firewall, Anti-virus, Anti-spyware software installed Training computer users on internet threats, to include phishing emails, and how to identify and report suspicious IT activity
Contact CBP Website	Processing CBP entry and receive immediate electronic CBP release	Brokerage Manager monitors the CBP release	Phishing through company internet access and email	IT Firewall, Anti-virus, Anti-spyware software installed Training computer users on internet threats, to include phishing emails, and how to identify and report suspicious IT activity
Contact CBP Website	Print CBP Forms	Entry processing	Storage of blank forms	All forms kept in locked cabinets or only available electronically on computer

Supply Chain Step	Type of Service Conducted by Our Company	Process	Risks Identified	Actions Taken to Mitigate Risks
Arranging Pickup and Delivery	Arrange pick-up and delivery by approved Trucker upon arrival of freight	Quality Assurance Department monitors the selection of Truckers	Selection of trucker not on approved list Use of outdated approved list	Ensure employees trained to use truckers only on current list posted on intranet (no hardcopies that may be outdated allowed)
Instructing selected Trucker	Notify Trucker to validate container number, inspect container and perform View, Verify, Tug, and Twist seal inspection	Brokerage Compliance Department monitors the notification to Truckers	Improper communication to the selected Trucker	Periodic audit of notification e-mail messages
Pick Up and Deliver Shipment	Dispatch trucker for Pickup and Delivery of shipment	Dispatching Brokerage Staff	Diversion of products for introduction/ removal of unauthorized materials	Use of escort, GPS and driver who calls dispatcher often to update on movements until delivery. Dispatcher who logs contacts with driver and conducts real-time comparisons to GPS data/ driver calls. Audits of tracking and monitoring records for anomalies
Contact with Consignee	Verify delivery and obtain Proof of Delivery	Brokerage Manager monitors the process	Modification of documentation to conceal wrong doing	Regular checking by Brokerage Manager
Contact CBP	Submission of entry summary for final reconciliation by CBP	Brokerage Manager monitors the process	Concealing wrong doing	CBP reconciliation detects anomalies
Closing and filing	Closing entry files and filing them away for records	Brokerage Manager monitors the process	Ensure prevention of leakage of documents	Regular documented auditing by Brokerage Manager
Destruction of Records	Destroying entry files, commercial invoices, email printouts, etc.	Use of on-site contract shredding truck	Ensure documents are actually destroyed and not diverted during process	All destruction is conducted under direct supervision of brokerage employee

Physical Security

If the company has a security alarm system:

- ☐ What was the date of the last system test?
- ☐ What were the results?
- ☐ What possible improvements were identified?

If the company has a video surveillance system:

- ☐ What was the date of the last system test?
- ☐ Does review of night time video show adequate lighting in place?
- ☐ Were repairs made immediately upon discovery of a malfunction?
- ☐ Was a verification conducted to ensure that security cameras remained pointed on key areas?
- ☐ Are cameras not easily accessible in order to prevent tampering?
- ☐ Are recordings stored in a secure location?
- ☐ Describe what issues were identified and actions taken to address issues:
- ☐ What actions were taken to improve processes in this security category?

Access Controls

Access Device Logs

- ☐ Did a review of the issuance/retrieval of access device logs reveal any discrepancies? (e.g. any ex-employees still shown as having keys, ID cards, alarm codes?)
- ☐ Was a physical inventory of all access devices conducted?
- ☐ If yes, what issues of concern were found?
- ☐ What actions were taken to resolve these issues?
- ☐ What actions were taken to prevent recurrences?

- ☐ Building Inspections
- ☐ Are building inspection logs complete?
- ☐ Were identified issues resolved?
- ☐ How can the process to ensure building integrity be improved?
- ☐ What actions were taken to improve processes in this security category?

Personnel

Review all personnel files of persons hired and separated since last assessment.

- ☐ Did the review show any documents or data missing or incomplete?
- ☐ Were I-9 forms complete?
- ☐ Were all new hires queried through the E-Verify system?
- ☐ What patterns emerged concerning missing documents or data?
- ☐ What actions were taken to prevent recurrences?
- ☐ What actions were taken to improve processes in this security category?

Security Awareness and Training

- ☐ Has security training been updated since the previous iteration?
- ☐ Have all employees received mandatory training for their job position?
- ☐ If no, has make-up training been scheduled?
- ☐ What security topics were covered, and was training tailored to the responsibilities/jobs of the employees?

Below find a sample log that can be kept to ensure each employee receives the necessary job-specific training.

Employee Name	Job Title	C-TPAT Program Criteria	17-Point Inspections	Documenting Inspections	Challenging Strangers	Abnormal Shipments	Reporting Suspicious Activities	Conducting Site Security	IT Security	Mail / Package Safety
Woods, Porter	Operations Clerk	[Date]	N/A	N/A	[Date]	[Date]	[Date]	N/A	[Date]	[Date]
Adams, John	Dispatcher	[Date]	[Date]	[Date]	[Date]	[Date]	[Date]	N/A	[Date]	[Date]
Fraser, Alex	Mechanic	[Date]	[Date]	[Date]	[Date]	N/A	[Date]	N/A	N/A	N/A
Foss, Joseph	Driver	[Date]	[Date]	[Date]	[Date]	[Date]	[Date]	[Date]	N/A	N/A

N/A — Not applicable, this employee does not perform this activity/task.
[Date] — Last date this training was completed by this employee.
All training should be refreshed periodically, *at least* annually.

Information Technology (IT)

- ☐ Has the IT service provider been rescreened since the initial contract was signed?
- ☐ How frequently are firewall, anti-virus, and anti-spyware software updated?
- ☐ Was a security intrusion test performed to determine the effectiveness of protections?
- ☐ What were the results?
- ☐ What can be improved?
- ☐ How frequently are system backups conducted?
- ☐ Are backups stored in secure location?
- ☐ If cloud storage is used, was business partner screening conducted on the provider?
- ☐ Has IT retraining been conducted and documented?
- ☐ What actions were taken to improve processes in this security category?

Chapter Three

U.S. CUSTOMS AND BORDER PROTECTION

Consolidator Partners in the C-TPAT program are not required to physically handle cargo, or even be involved in the import process. Consolidators who otherwise meet the C-TPAT eligibility requirements may be involved solely in the export business. Thus, many potential business models for C-TPAT consolidators exist. When determining how to create a Risk Assessment Process, consolidators should consider their business model first. For a consolidator, steps one through three of the five step process could vary widely depending on the company's business model.

1. Cargo Mapping

- Cargo handler (foreign or domestic) — similar to importer and exporter
- Non-cargo handler — similar to broker

2. Vulnerability

- Cargo handler (foreign) — similar to foreign manufacturer
- Cargo handler (domestic) — similar to importer and exporter
- Non-cargo handler — similar to broker

3. Threat

- Cargo handler (foreign) — similar to foreign manufacturer
- Cargo handler (domestic) — similar to importer and exporter
- Non-cargo handler — similar to broker

4. Action Plan

5. Documented Procedure

If the company does not physically handle freight, instead functioning primarily as a freight forwarder or "paper" consolidator, the Broker Risk Assessment model may best apply. If the consolidator is physically handling imported freight, the importer model may apply, with modifications. For export-only consolidators, a risk assessment process closer to that of a U.S. exporter may apply. For consolidators that also control the operations at a foreign facility for cargo moving to the U.S., concepts from the foreign manufacturer risk assessment process may be most applicable.

Obviously, consolidators are not typically in the business of selecting foreign manufacturers or foreign incountry transportation providers. Manufacturers are typically selected by the consolidator's client-importer, and foreign in-country transportation providers are often selected by the consolidator's foreign business partner agents. To address this lack of control over selecting business partners, it is extremely important for consolidators to address risk by selecting quality foreign agents, and to have strong and proactive outreach and education programs on C-TPAT and equivalent AEO programs. "Pushing out" the C-TPAT minimum security criteria to all levels of the supply chain through outreach and education, including to third and fourth level business partners, is a critical minimum security criteria element for all C-TPAT Partners, and becomes especially important when Partners have limited ability to select transportation providers in foreign countries. The best-case scenario is to require all partners in all links in the supply chain to be AEO or C-TPAT certified.

As an example of the dangers of using generic, "cookie cutter" risk assessments, consider a consolidator that does not handle cargo and has a single office located in a high-rise office building, but has elected to use a generic risk assessment process provided by an external advisor. The only valuable item such a consolidator possesses is information, but the generic process adopted from their advisor is actually formulated for importers who physically handle their own cargo.

Now consider these vulnerabilities:

- A third-party janitorial service, selected by the building landlord, has metal keys allowing access for cleaning on Sundays when the consolidator's office is closed.
- The consolidator has no alarm system to record when the third party employees, who are completely unknown and unscreened by the consolidator, actually enter and exit the office space.
- The consolidator assumes the janitors access the office only on Sunday evenings, but have no method to verify this.
- No video camera system exists for the consolidator's managers to review each morning to determine who was in the office after hours, and what they were doing.
- The office photocopier's electronic records are not reviewed to determine if photocopies are made outside normal office hours.
- The consolidator's IT contractor conducts no special checks or reports to determine if the company's IT system has been accessed or used outside normal business hours.

While the company has established a Risk Assessment process, it does not fit the company's business model and can lead to a false sense of security and eventual data theft. Is this the type of business partner with whom you would willingly put your personal bank account or company identity information at risk?


CAUTION
CAUTION

Chapter Four

U.S. CUSTOMS AND BORDER PROTECTION

Cross-border highway carriers' business models have some similarities to brokers, in the sense both brokers and carriers are hired by importers or manufacturers to provide services to these clients. However, while brokers need only protect a set location or locations, carriers, by their very nature, must be able to protect stationary facilities and moving conveyances.

For highway carriers, a supply chain might be displayed as the sample below.

Supply Chain Step	Type of Activity	Details About Partner	Issues to Consider
Foreign Manufacturer	Trailer storage, trailer loading	ABC Manufacturer, 123 Chavez, Tijuana, Baja California, provides 53% of shipments we move to US.	C-TPAT Certified, Physical security around truck and trailer (fences, gates, guards); restricted access to loading dock; secure overnight storage
Transport to border	Movement of cargo from manufacturer to border. Loaded trailers never taken to our storage yard.	This is our company. Internal procedures, especially as related to tracking and monitoring, must address vulnerabilities.	Tight and overlapping tracking and monitoring of trucks must be in place, with direct management oversight and written procedures for when things go wrong.
Export broker	Company that provides border crossing paperwork and may transmit data to government agencies.	Mexico broker. Knows about shipment and details in advance.	Are Personnel and IT security at a high level?
Port of Entry to US	Wait time	What is typical wait and release time at each port of entry?	How exposed is conveyance while waiting in line?
US Import broker	Company that provides border crossing paperwork and may transmit data to CBP.	US broker. Knows about shipment and details in advance.	Are Personnel and IT security at a high level?
Transport to destination in US	Movement of cargo from border to destination/transfer yard.	This is our company. Internal procedures, especially as related to tracking and monitoring, must address vulnerabilities. Reporting delays and suspicious activities critical for driver.	Tight and overlapping tracking and monitoring of trucks must be in place, with direct management oversight and written procedures for when things go wrong.

Once locations and movements are identified, the regional Threat Assessment can be applied against these steps in the carrier's daily activities to determine where weaknesses and vulnerabilities exist. Once these vulnerabilities are identified, an Action Plan to address such issues can be documented. A highway carrier's risk assessment will have more to do with addressing internal processes and vulnerabilities at points of loading, as opposed to correcting weaknesses in clients' internal processes, as the highway carrier is the service provider. Nevertheless, there may come a time when a client's processes are so high risk the highway carrier may determine for its own safety to stop conducting business with that client.

Highway carriers that handle less than trailer load freight and a spoke and hub consolidation network will have a different set of issues to address than in the example above. Similarly, carriers using a pick up and deliver ("milk run") business model will have a more complex series of issues to consider.

Risk factors for Highway Carriers

The history of highway carriers in the C-TPAT Program has demonstrated the issues below as being repetitive contributors to security breaches. Therefore, each step in a carrier's supply chain and business model should be analyzed for weaknesses in these areas:

- Loose tracking and monitoring of conveyances in transit;
- No overlapping or layered verifications of conveyance monitoring (e.g. no GPS to go with radio communications with drivers, no unannounced following of conveyances by managers, no escorts or convoys in use, etc.);
- Weak oversight at office of tracking and monitoring procedures (e.g. dispatcher over-burdened, improperly trained, not rotated randomly to avoid collusion with drivers)
- Use of subcontractors;
- No direct management oversight in day-to-day operations;
- Inappropriate delegation of authority to employees (e.g. allowing dispatchers to choose or approve clients and other business partners);
- No or weak use of GPS and geo-fencing;
- Infrequent visits to business partners at point of loading to discuss and inspect security;
- Security where loaded and empty conveyances and tractors are stored overnight;
- If drivers must leave vehicle to pick up paperwork en route;
- Time elapsed since last full investigation/check of driver (not simply DOT drug tests)
- Employee turnover rate at business partners; and
- No C-TPAT/PIP/NEEC participation, even though eligible.

U.S. CUSTOMS AND BORDER PROTECTION

Chapter Five

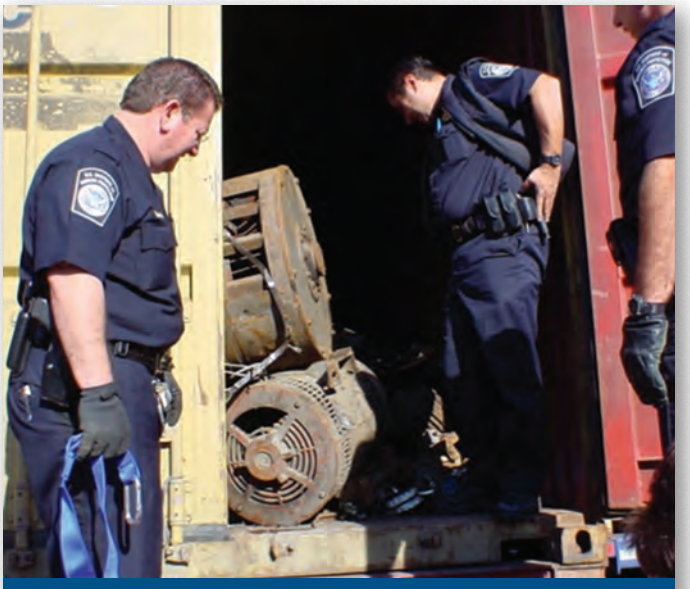
Where a manufacturer outsources or contracts elements of their supply chain, such as another facility, warehouse, or other elements, to include transportation, the manufacturer must work with these business partners to ensure pertinent security measures are in place and are adhered to throughout their supply chain. The supply chain for C-TPAT purposes is defined from point of origin through to point of distribution.

Manufacturers and exporters are often responsible for selecting the carriers for freight destined to the port of export, and frequently across the border to destination as well. Other partners in the export chain might also be selected by the manufacturer or exporter, such as freight forwarders, brokers, consolidators, etc. As selecting these service providers is the responsibility of manufacturers and exporters, so too is screening these business partners to ensure such partners are meeting the C-TPAT minimum security criteria. The easiest method, of course, is to select partners who are C-TPAT Partners and/or members of other governments' supply chain security programs. If a business partner has no such certification, then the manufacturer or exporter must conduct security assessments of all such business partners in the supply chain.

The table on the following pages is an example of how a manufacturer exporting to the U.S. might document their supply chain.

Compartment in Trailer Floor

Supply Chain Step	Type of Service Provided	Details About Business Partner	Issues to Consider
Manufacturer	Manufacturing/Exporter	This is our company, Francisco Javier Clavijero	C-TPAT Certified
Highway Carrier (for both FCL and LCL)	Moves cargo from factory to port of export	Pedro Thomas Ruiz de Velasco	C-TPAT Status Verified in Portal
Export Broker	Processes paperwork for cargo export	José Guadalupe Posada	NEEC Eligible, application in process
U.S. Port of Entry	Wait time	What is typical wait and release time?	How exposed is conveyance while waiting in line?
U.S. Broker	Files import documentation at destination	Jose Mendoza Brokers	Not C-TPAT, but eligible. Why not C-TPAT? Investigation and Security Assessment must be conducted. Are Personnel and IT security at a high level?
Transport to destination in U.S.	Movement of cargo from border to destination/ transfer yard.	This is our company. Internal procedures, especially as related to tracking and monitoring, must address vulnerabilities. Reporting delays and suspicious activities critical for driver.	Tight and overlapping tracking and monitoring of trucks must be in place, with direct management oversight and written procedures for when things go wrong.
Importer/Consignee	U.S. Importer client	Agerholm Importers 524 Mesquite Drive, Laredo, Texas	C-TPAT Status Verified in Portal



Export Examination

Below is an example of how a U.S. exporter might document their supply chain.

Supply Chain Step	Type of Service Provided	Details About Business Partner	Issues to Consider
Manufacturer	Exporter	This is our company, Henderson Manufacturers	C-TPAT Status Verified in Portal
Highway Carrier (for both FCL and LCL)	Moves cargo from factory to port of export	Wilson Trucking, 231 Dean Forest Rd., Savannah, GA	Not eligible. Security Assessment for this year on file. Working with company to activate five minute pings and geo-fencing on GPS system.
Freight Forwarder	Processes paperwork for cargo export	Global Freight Coordinators, 21 Bay St., Savannah, GA	Not eligible, but could be if they obtained CBP bond. Outreach to partner should be conducted to encourage C-TPAT participation.
Port of Export	Stores and handles cargo prior to lading	Georgia Port Authority	C-TPAT Status Verified in Portal
Ocean Carrier	Moves cargo from port to port	Excellent Ocean Carriers	C-TPAT Status Verified in Portal
Transhipment Port	Stores and handles cargo in between vessel movements	Izmir, Turkey	No, but could apply to C-TPAT
Ocean Carrier	Moves cargo from port to port	Mersin Carriers	Not eligible
Port of Entry at Foreign	Location of unlading	Constanta, Romania	No, but could apply to AEO. Romanian client asked to conduct outreach and encourage membership.
Foreign Broker	Files import documentation at destination	Torenescu Brothers	No, but could apply to AEO. Romanian client asked to conduct outreach and encourage membership.
Terminal Operator	Handles and stores cargo after unlading	Constanta Government Terminal	No, but could apply to AEO. Romanian client asked to conduct outreach and encourage membership.
Foreign Drayage	Trucks cargo from ocean terminal to destination	Ponta Transport	Not eligible, completed security questionnaire for this year on file
Foreign Consignee	This is our client.	Basescu Importers	AEO Certified, Certificate on file in Document Exchange

U.S. CUSTOMS AND BORDER PROTECTION

U.S. Customs and Border Protection

U.S. Customs and Border Protection
Office of Field Operations
C-TPAT Program
1300 Pennsylvania Avenue, NW
Washington, DC 20229

(202) 344-1180
industry.partnership@dhs.gov

Please visit the CBP and C-TPAT Web sites at
www.cbp.gov
www.cbp.gov/ctpat

CBP Publication No. 0206-0814
August 2014