Supply Chain Security Risk Assessment Frequently Asked Questions

In an effort to clarify the April 23, 2010 bulletin regarding international supply chain security risk assessments, C-TPAT offers the following Frequently Asked Questions (FAQ) to provide further guidance. C-TPAT appreciates member involvement in developing these FAQ's and the positive dialogue established on this important subject which is fundamental to the core principles of the program. Specific questions / guidance on how your company should approach an international supply chain security risk assessment process based on your business model should be discussed with your company's assigned supply chain security specialist. This document will be available in the web portal Public Document Library as well as on the C-TPAT website.

Q: What prompted the need to clarify C-TPAT's expectations with respect to an International Supply Chain Security Risk Assessment?

A: The C-TPAT program has continued to evolve since its inception. During the validation / revalidation process and when conducting an in-depth review of security breaches, it became apparent that the process of conducting an international supply chain security risk assessment was not being performed completely. Most C-TPAT members are conducting a comprehensive domestic risk assessment of their own facilities and processes in the United States; however, many members were not assessing the potential threats and vulnerabilities that may exist within their international supply chain from the point of packing / stuffing and at each transportation link within the chain, until the cargo reaches the final point of distribution in the United States.

Q: What is an International Supply Chain Security Risk Assessment?

A: An International Supply Chain Security Risk Assessment examines security threats and vulnerabilities associated with a C-TPAT member's international supply chain, from the point of origin where the goods are packed / stuffed, until they reach their final destination for distribution. A Security Risk Assessment is a fundamental part of a company's security program.

Q: Is an International Supply Chain Security Risk Assessment a new requirement for C-TPAT members?

A: No. The components of an International Supply Chain Security Risk Assessment are identified throughout the C-TPAT minimum security criteria, particularly in the preamble to the importer minimum security criteria and under the Business Partner Requirements and Security Procedures sections. C-TPAT minimum security criteria outline the requirements each C-TPAT member must or should adhere to in order to participate in the program.

Q: When should an International Supply Chain Security Risk Assessment take place?

A: Prior to applying to the C-TPAT program, applicants must conduct a comprehensive assessment of their international supply chain(s) in order to meet the minimum security criteria for the program. C-TPAT members must conduct a comprehensive assessment at least annually in order to remain in the C-TPAT program.

Q: What guidance does the C-TPAT program offer members to assist companies in conducting an International Supply Chain Security Risk Assessment?

A: The C-TPAT program has developed a basic "5 Step Risk Assessment Process Guide" to assist members in conducting an international security risk assessment of their international supply chain(s). The guide can be found in the C-TPAT web portal Public Document Library.

Q: What does the "5 Step Supply Chain Security Risk Assessment Process" consist of?

A: Mapping Cargo and Business Partners: Identify Business Partners 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).

Conducting a Threat Assessment: Identify such threats as Terrorism, Contraband / Human Smuggling, Organized Crime, or other Conditions which may increase the probability of a security breach.

Conducting a Security Vulnerability Assessment: Based on C-TPAT minimum security criteria, determine if Business Partners have gaps, vulnerabilities, or weaknesses which may lead to a security breach.

Preparing an Action Plan to Address Vulnerabilities: Developing a written strategy to address potential gaps, vulnerabilities, and weaknesses.

Documenting How the Security Risk Assessment is Conducted: Writing the policies / procedures on who will be responsible for conducting the assessment; what will be included in the

assessment; why the assessment must be conducted; when (how often) the assessment will be conducted; where the assessments will be conducted; and how the assessment will be conducted.

Q: Is my company required to use the "5 Step Risk Assessment Process Guide"?

A: No. The C-TPAT program clearly understands there are a wide variety of business models and the "5 Step Risk Assessment Process" may not fit all business models. However, the C-TPAT program expects its members to have a documented process for determining and addressing security risks throughout their international supply chains, as outlined in the minimum security criteria. The "5 Step Risk Assessment Process Guide" was developed to clarify C-TPAT program expectations regarding what should be included in an international supply chain security risk assessment. In addition, the guide was developed to provide basic tools, resources, and examples in order to assist members in conducting a comprehensive supply chain security risk assessment of their international supply chain(s).

Q: If my company has a large number of supply chains, does C-TPAT expect me to perform the entire 5 Step Risk Assessment Process for all of my company's supply chains, including completion of Step 3 – Conduct Vulnerability Assessment and Step 4 – Prepare Action Plan?

A: No. The C-TPAT program expects its members to identify "High Risk" supply chains based on the following security threats at the point of origin:

- Terrorism;
- Contraband Smuggling;
- Human Smuggling;
- Organized Crime; and
- Conditions fostering the above threats.

Members must determine if security vulnerabilities exist with key Business Partners in those "High Risk" supply chains through means such as verifying C-TPAT membership (if eligible), verifying certification in an equivalent security program administered by a foreign Customs authority or through security surveys / questionnaires / site visit verifications, etc.

Members may also wish to consider reviewing "high volume" supply chains and / or Business Partners with whom they have experienced other security issues (e.g., theft, inaccurate manifesting, transportation monitoring / tracking problems, etc.) that are not necessarily operating in "High Risk" environments.

Q: Regarding the Status Verification Interface (SVI) numbers for Business Partners that are already in C-TPAT, will C-TPAT members be required to obtain risk assessment information from those Business Partners, instead of simply verifying their SVI number? In the past, the requirement has been for importers to verify and monitor SVI numbers, but not to conduct deeper security assessments if the Business Partner is certified.

A: No, C-TPAT members will not be required to obtain risk assessment information from their C-TPAT Business Partners that are already in good standing (i.e. Certified) in the program. C-TPAT members should continue to verify the status of their Business Partners utilizing the SVI system within the C-TPAT web portal.

Q: What is an importer's responsibility regarding vulnerability assessment of non-importers in their international supply chain(s) (i.e. should an importer assess the vulnerability of their Business Partners against the minimum security criteria for importers)?

A: The importer member is responsible for ensuring that all their Business Partners are either C-TPAT certified or comply with the C-TPAT minimum security criteria. One technique to ensure compliance for non C-TPAT Business Partner is to use the C-TPAT minimum security as a guide to conduct the vulnerability assessment. For example, if the non C-TPAT Business Partner is a manufacturer, the importer may complete a vulnerability assessment of the company using the Foreign Manufacturer minimum security criteria. If the non-C-TPAT Business Partner is a highway carrier, then the importer could complete a vulnerability assessment of the company using the Highway Carrier minimum security criteria.

Q: Are all C-TPAT members (importers, brokers, consolidators, carriers, etc.) expected to conduct an international supply chain security risk assessment?

A: Yes. However, some Business entities may need to modify the "5 Step Risk Assessment Process" to fit their Business model. For example, an international supply chain security risk assessment for a broker, carrier, or consolidator who has hundreds of clients may identify and focus on supply chains where threats are high (terrorism, contraband / human smuggling, etc.) and incorporate an appropriate vulnerability assessment into their customer screening process. For example, customer screening may consist of a questionnaire with questions to help determine the legitimacy of the client's Business and measures to secure their cargo at the point of origin.

Q: Are small companies required to conduct a Supply Chain Security Risk Assessment?

A: Yes. All C-TPAT members are required to conduct a Supply Chain Security Risk Assessment of their international supply chain(s). All C-TPAT members are expected to have a documented process for determining and addressing security risks throughout their international supply chain(s) in order to meet the minimum security criteria. C-TPAT recognizes that not all supply chains are alike and the extent to which a risk assessment is performed will vary depending upon the complexity of the factors involved. The key point is that members need to take a proactive approach to address risk in their supply chains.

Q: Is it necessary to have a numerical rating system to quantify risk or can an alternative method to assess risk (e.g. Acceptable / Unacceptable) be used?

A: No, it is not necessary to use a numerical rating system to assess risk: an alternative method can be used. It is up to each company to determine how risk will be assessed. The threat and vulnerability factors outlined in the "5 Step Risk Assessment Process Guide" should be used to determine the level of risk (high-medium-low, acceptable-unacceptable, pass-fail, etc.). A complex rating system is not appropriate for all Business models.

Q: Can CBP advise what the standard for determining whether a "Security Risk Assessment" is adequate in order to meet the minimum security criteria?

A: Following the "5 Step Risk Assessment Process Guide" to the greatest extent possible will help ensure the C-TPAT member's risk assessment adequately addresses the minimum-security criteria. Recommendations may be made by or sought from the assigned Supply Chain Security Specialists to enhance the supply chain security risk assessment process, based on the company's size and Business model.

Q: As a C-TPAT importer, do "incoterms" dictate when I become responsible for security within the international supply chain? For example, if I am a C-TPAT certified importer and purchase cargo Landed Duty Paid (LDP) or Delivered Duty Paid (DDP), am I required to conduct an international supply chain security risk assessment? What if I am the ultimate consignee and receive goods from a C-TPAT certified importer?

A: No, incoterms do not dictate when an importer member becomes responsible for security within the international supply chain as a C-TPAT member. C-TPAT importer members are responsible for securing cargo from the point of packing / stuffing, until the cargo reaches its final destination point for distribution in the United States, regardless of incoterms for the shipment.

If a C-TPAT importer member directly caused the shipment to be imported into the United States by issuing a purchase order or through another established business process and is clearly aware the goods will be sourced / manufactured and imported on their behalf, the member is responsible for ensuring the cargo is secure. No matter when the importer becomes the legal owner of the shipment, if the importer directly caused the shipment to come to the United States, the importer is responsible for conducting a risk assessment. C-TPAT minimum security criteria "Business Partner Requirements" outline this requirement. In the instance where the C-TPAT member is the ultimate consignee, confirming that the importer is a C-TPAT certified member will normally meet the program's expectations. However, C-TPAT encourages members to coordinate with one another in such instances to ensure no gaps exist and responsibilities are clearly identified.