U.S. Customs and Border Protection

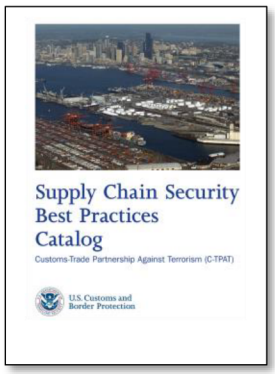
CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

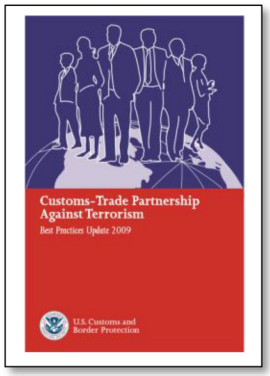
Customs Trade Partnership Against Terrorism

Best Practices Framework

Last Updated: July 20, 2021

In 2006, the Customs Trade Partnership Against Terrorism (CTPAT) program published the *Supply Chain Security Best Practices Catalog* in an effort to provide Members with up to date information on highly effective cargo security practices identified by CTPAT Supply Chain Security Specialists (SCSS) while conducting validations. Over the next three years, many of the best practices identified in this catalog essentially became industry standards. This led the program to issue the *2009 Best Practices Update*, a pamphlet that identified new best practices in supply chain security in each of the eight minimum security criteria (MSC) categories that existed in the program back then.





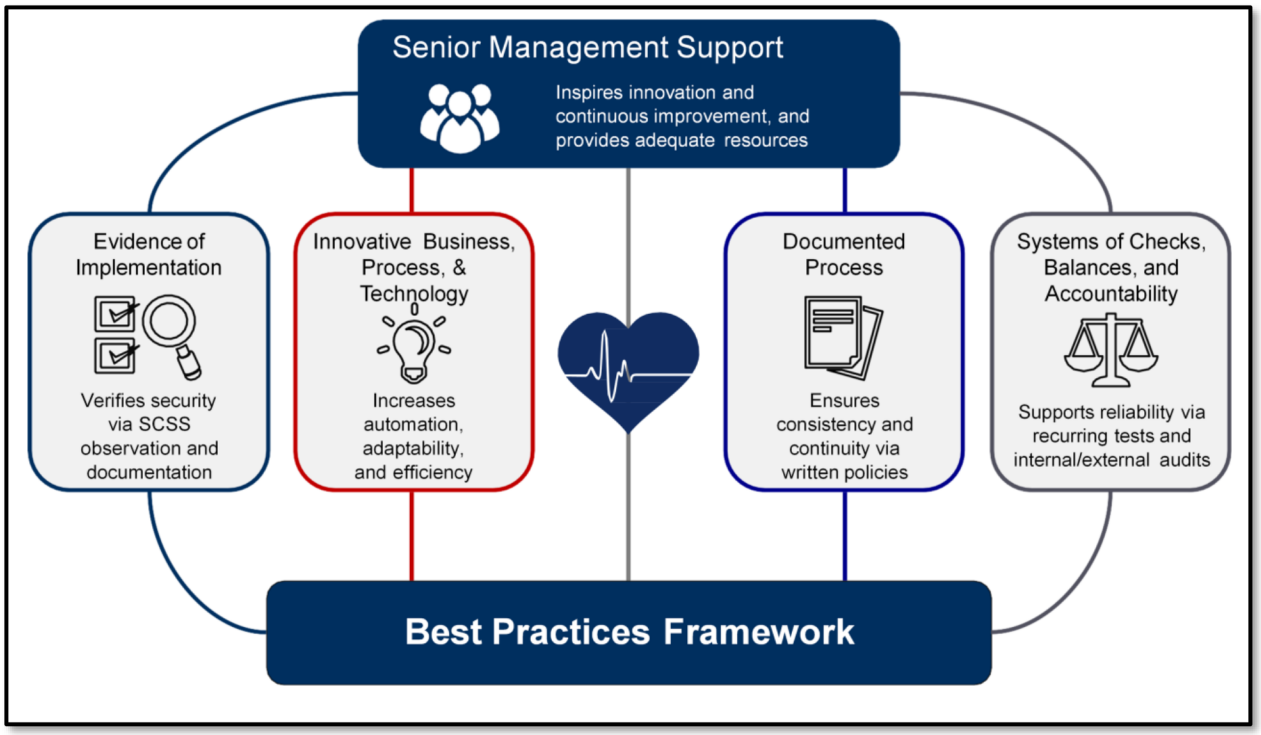
This meant that Members exceeded the MSC by complying with specific lists of best practices that the program published. CTPAT Members then used the catalog to pick up best practices without really demonstrating that they were in fact meeting any particular set of standards – a framework.

In consultation with the trade, the program determined in 2017 that a best practices framework created a more agile and effective process, since a framework – as opposed to a prescriptive list – allows companies to identify or build specific and unique best practices. Another particular advantage of the framework is that it is scalable – it can be adopted by any company, including small and medium size enterprises.

A CTPAT Best Practice - A security measure which has senior management support to promote and sustain it. The measure is innovative for the Member's business model/size, verifiable through documented/observable evidence of implementation, and is tested/audited for its effectiveness.

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

For CTPAT purposes, a best practice must meet all five of the following requirements, all of which are subject to verification by the CTPAT Supply Chain Security Specialist.



1. **Senior Management Support** – A security measure that has senior management support to promote and sustain it.

    - Inspires/encourages innovation and continuous improvement.
    - Ensures financial support/resources are available to implement and maintain a robust security measure (staffing, training, technology, equipment, etc.).
    - Provides incentives/recognition to maintain high levels of security (not necessarily monetary!).
    - Integrates security measures into existing business processes.

2. **The measure is innovative for the Member's business model/size –** The security measure incorporates:

    - Automation to improve its effectiveness.
    - Technology to improve a process, checks, balances, and accountability.
    - Streamlined process to increase transparency in order to quickly detect anomalies.

3. **Documented process** – To ensure consistency and continuity, the process to carry out the security measure must be documented (written), to include one or more of the following, as appropriate to business model/size:

   - Policy
   - Procedures
   - Work Instructions
   - Checklists

4. **System of Checks and Balances** – To ensure the reliability of the security measure, the member must have implemented a regular and recurring system of documented checks, balances, and accountability that incorporates one or more of the following measures:

   - Internal and external tests supported by corrective action plans and follow-up monitoring based on results to the corrective actions.
   - Internal and external audits supported by corrective action plans and follow-up monitoring based on results to the corrective actions

5. **Evidence of Implementation** – The Member has met all the security requirements of the program and evidence has been verified by the Supply Chain Security Specialist that the innovative business process or technology has been implemented. This verification may be done during the validation process or through document reviews or both.

Tier III – CTPAT Importers and Exporters

CTPAT Importers and Exporters may go from Tier II status (Certified-Validated) to Tier III (Certified - Exceeding) if they meet the following requirements:

- Meet the minimum security criteria;
- Have successfully undergone a CTPAT validation with no actions required; and,
- Have successfully demonstrated to its CTPAT Supply Chain Security Specialist that it has implemented at least one best practice per the Best Practices Framework.

CTPAT hopes to extend the opportunity to other entities in the supply chain – such as carriers – to become Tier III in the future.

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW - Washington, DC 20229