CTPAT - Minimum Security Criteria (MSC) Update

U.S. Customs and Border Protection

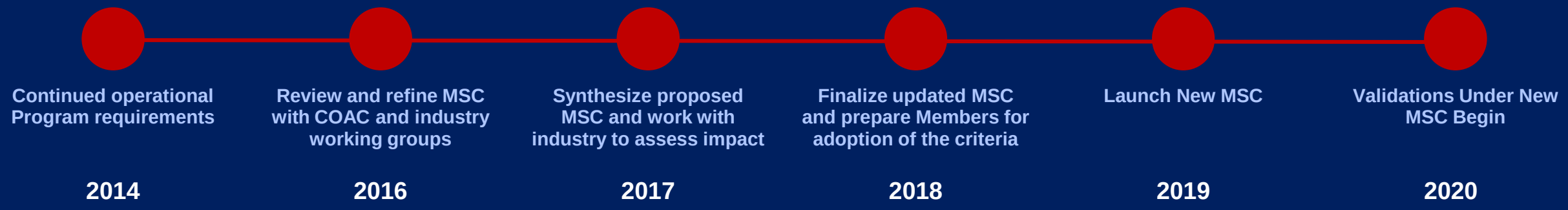
Carlos E. Ochoa
Branch Chief – Trade Engagement and Communications

CTPAT Conference 2019

CTPAT MSC Update

Over the past two and a half years, CTPAT conducted the first-ever review and update of its Minimum Security Criteria (MSC) in close cooperation with the Trade. This process involved:

- Early 2016 – MSC Working Group Created Under COAC
- WG: Made up Six Teams / Each Addressing a Specific Set of Proposals
- Teleconferences, Webinars, Face to Face Meetings: Reach Consensus
- October-December 2018 - Socialization Period with the trade at large — Over 800 comments received
- May 2019 – New MSC Released



MSC Working Group Members

Dave Berry – Swift
David Blackorby – Walmart Inc.
Barry Brandman – Danbee Investigations
Stella Bray-Conrad – Walmart Inc.
Bob Byrne – IBM Corporation
Fermin Cuza – World BASC Organization
Lana Dresen – S.C. Johnson and Son
Lenny Feldman – Sandler & Travis
Ray Fernandez – Sealock Security Systems, Inc.
Chuck Forsaith – Healthcare Distribution Alliance -
Pharmaceutical Cargo Security Coalition
Brandon Fried – Air Freight Forwarders
Lisa Gelsomino – Avalon Risk Management
Kathryn Gunderson – Boeing Company
Kevin J. Hayes – Long Beach Container Terminals
Vincent Iacopella – Alba Wheels Up

Alan Kohlscheen – IBM Corporation
Eugene Laney – DHL U.S.
Alexandra Latham – COSTCO Wholesalers
Liz Merritt – Airlines for America
Dan Meylor – Carmichael
Theo Miles – Walmart Inc.
Kathy Neal – Regal Beloit Corporation
Kirsten A. Provence – Boeing Company
Dan Purtell – British Standards Institute
Adam Salerno – U.S. Chamber of Commerce
Doug Schneider – World Shipping Council
Lisa Schulte – Target Corporation
Beverley Seif – Mohawk Global Trade Advisors
Michael White – Intl. Air Transportation Association
David Wilt – Xerox Corporation
Jim Yarbrough – British Standards Institute
Michael Young – Orient Overseas Container Line

CTPAT – Strengthening the MSC

MSC Update Addresses Evolving Challenges and Threats.

Legal Mandates	Reflect CBP's Mission	Changing Trade Landscape	CTPAT's Experience	Terrorism and Criminal Activity
SAFE Port Act TFTE Act – 2015 Reauthorization Bill (HR 3551)	2003 – New Federal agency, expanded mission.	Since 2001, trade volume has increased and technology plays a much greater role in how we conduct trade.	New MSC reflect lessons learned	Supply chain targeted by ever evolving threats

CTPAT MSC – Clarity

New MSC Structure – Adopted by the MSC Working Group put together under the umbrella of the COAC.

- **New Focus Areas & Criteria Categories**

  Established **3 focus areas**, inclusive of **three new criteria categories:** Security Vision and Responsibility, Cybersecurity, and Agricultural Security

- **Must vs Should Requirements**

  Clarified language to explicitly organize criteria into **"Musts" and "Shoulds"** – requirements and recommendations.

- **Implementation Guidance**

  For the first time, criteria is supported by Implementation Guidance – **additional background to the criteria** to assist the member understand and implement the MSC.

The Basics – What is a Standard?

ISO - A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.

- Level of quality or attainment / Rise to the Standard
- Knowledge - Distilled wisdom of people with expertise in the subject matter and who know the needs of the organization they represent.
- They are designed for voluntary use.

Examples: BASC, SCAN, TAPA, ASIS

MSC – Performance v. Prescriptive

Performance vs. Prescriptive

A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the regulated entity.

In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance standard sets a goal and lets each regulated entity decide how to meet it.

Prescriptive Benefits: Clarity / Uniformity / Transparency.

CTPAT- MSC Structure

FOCUS AREAS	CRITERIA CATEGORY NUMBER	CRITERIA CATEGORIES
I. Corporate Security	1	Security Vision and Responsibility
	2	Risk Assessment
	3	Business Partner Requirements
	4	Cybersecurity
II. Transportation Security	5	Conveyance and IIT Security
	6	Seal Security
	7	Procedural Security
	8	Agricultural Security
III. People & Physical Security	9	Physical Access Controls
	10	Physical Security
	11	Personnel Security
	12	Security Training, Threat, and Awareness

3 Focus Areas

12 Security Criteria Categories

Each Criterion Has an ID Number

MSC Categories – Security Vision and Responsibility

New Category: Supply chain security must become an integral part of a company's culture and it must be incorporated into its core business processes.

Section 1 of the MSC – 4 Criteria – All Core

Organizational culture and management philosophy which:

- Promotes a culture that encourages and demands a commitment to compliance with the law.
- Promotes security as a company-wide objective and responsibility.
- Outlines responsibilities for compliance, detailing internal controls, auditing practices, documentation policies, and disciplinary procedures.
- Recognizes the importance of the role that the company POC plays within the company and with CBP.

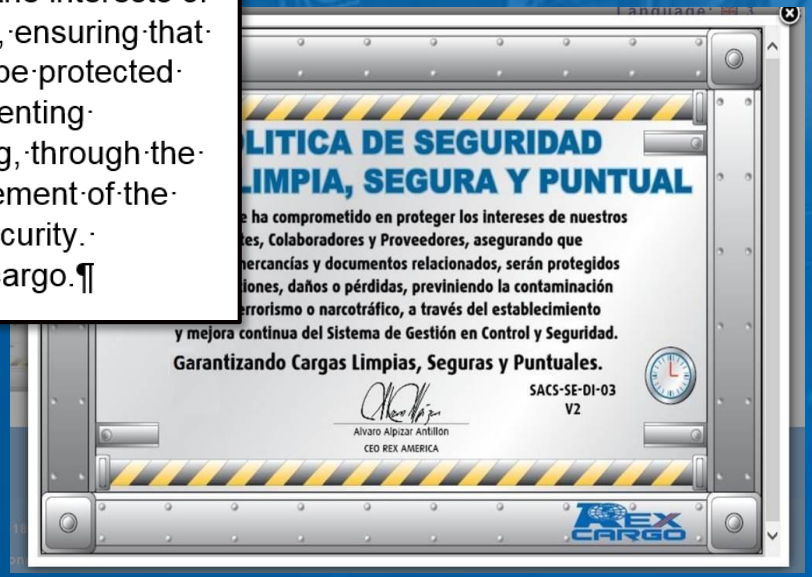
MSC Categories – Security Vision and Responsibility

Statement of Support – 1.1 - Should

REX CARGO
a Rex America Company

Security·Policy:¶

Rex·Cargo·is·committed·to·protecting·the·interests·of·our·customers,·partners·and·suppliers,·ensuring·that·all·goods·and·related·documents,·will·be·protected·from·alterations,·damage·or·loss,·preventing·pollution·by·terrorism·or·drug·trafficking,·through·the·establishment·and·continuous·improvement·of·the·management·system·in·control·and·security.·Ensuring·clean,·secure·and·punctual·cargo.¶



U.S. CUSTOMS AND BORDER PROTECTION

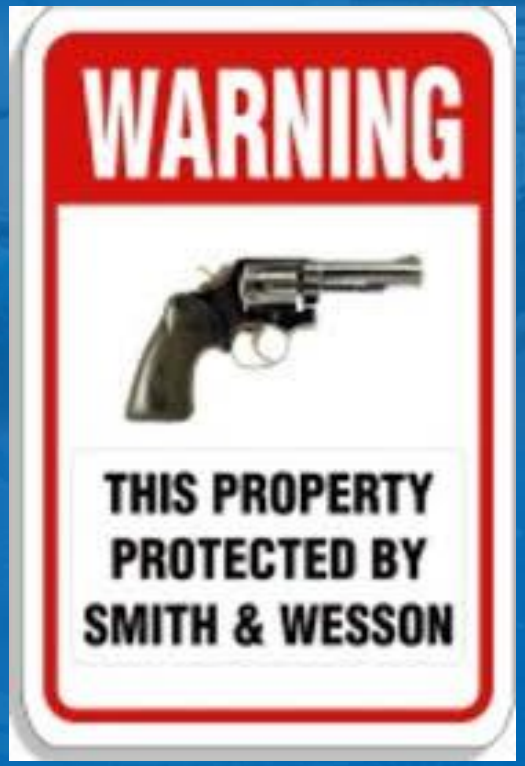
CORE VALUES

Vigilance
is how we ensure the safety of all Americans. We are continuously watchful and alert to deter, detect and prevent threats to our nation. We demonstrate courage and valor in the protection of our nation.

Service to Country
is embodied in the work we do. We are dedicated to defending and upholding the Constitution of the United States. The American people have entrusted us to protect the homeland and defend liberty.

Integrity
is our cornerstone. We are guided by the highest ethical and moral principles. Our actions bring honor to ourselves and our agency.

MSC Categories – Security Vision and Responsibility



MSC Categories – Security Vision and Responsibility

Proactive Role of Management Accentuated Throughout the Criteria:

- Risk Assessment: Crisis management / recovery plans / business resumption.
- Business Partners: Signature of manager on security questionnaires.
- Conveyance/IIT: Management conduct random searches of conveyances; random audits of tracking and monitoring procedures.
- Seal: Management conduct audits of seals.
- Procedural: Random screenings of driver's belongings.
- Physical: Periodic, random review of camera footage.

MSC Categories – Security Vision and Responsibility

Case Study – Air Environment Seizures

Contributing Factors:

- Lack of management oversight and accountability
- Complacency
- Not following company security policies and procedures
- Lack of monitoring company equipment and assets

Result

- Deeply entrenched internal and external conspiracy network which involved cleaning crews, caterers, mechanics, baggage handlers, and security personnel – who served as lookouts.

MSC Categories – Security Vision and Responsibility

Company CTPAT POC Knowledgeable About CTPAT – 1.4 - Must

In FY 2013 – 114 Members Removed

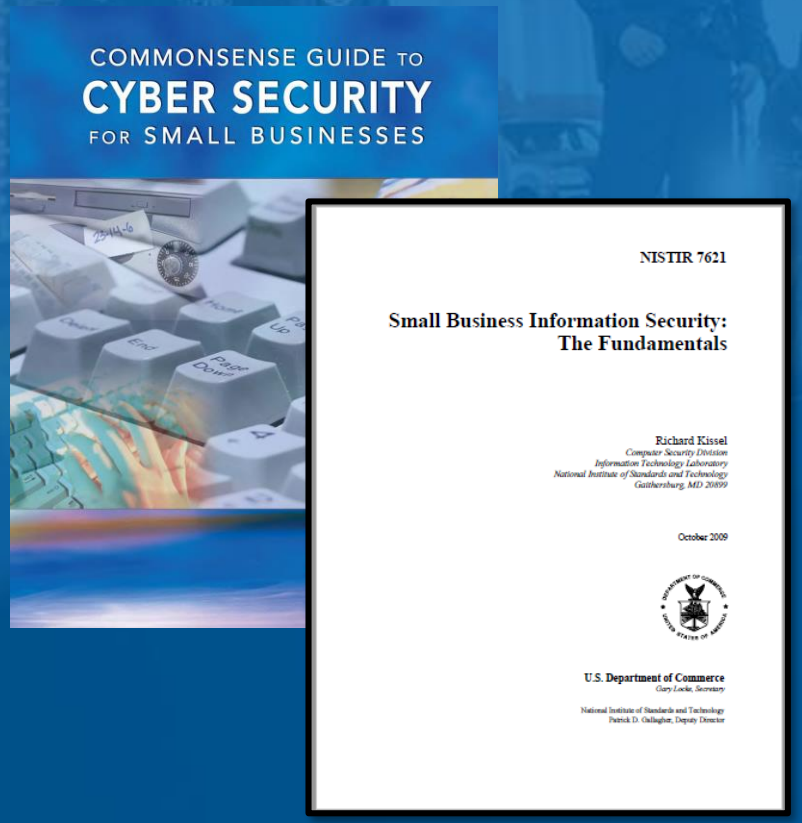
- Failed to respond to validation report: 53 (46.5% of total removals)
- Failed to complete annual self-assessment or security profile update: 31 (27.2% of total removals)
- Failed to meet commitment (e.g., failed to work with the SCSS to schedule a validation): 2
- Security breach: 7

MSC Categories – Cybersecurity

New Category: Cybersecurity is the key to safeguarding a company's most precious assets – intellectual property, customer information, financial and trade data, and employee records.

Section 4 of the MSC – 13 Criteria – All Core

Common sense criteria based on industry recommendations / Extend to Business Partners



U.S. National Cyber Security Alliance - 60% of small companies are unable to sustain their business more than six months following a cyberattack. They frequently just don't have the resources

NIST Interagency Report (NISTIR) 7621 - *Small Business Information Security: The Fundamentals* - Because small businesses typically don't invest in information security the way larger businesses can, many cybersecurity criminals view them as soft targets.

MSC Categories – Cybersecurity

National Institute of Standards and Technolgy – NIST : Cybersecurity supply chain risks caused by:

- Inferior information security practiced by lower tier suppliers.
- Third party service providers and vendors that have virtual access to information systems.
- Compromised hardware and software.

Examples: Netflix, Equifax, Panama Papers / Verizon's *2018 Data Breach Investigations Report*

MSC Categories – Cybersecurity

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

MSC Categories – Cybersecurity

Use of software/hardware to protect IT systems – 4.2 – Must

- Software to protect against malware
- Use of virus protection software program required on every workstation
- Firewalls – Shield computer from outside attacks or unnecessary network traffic.
- Recover following an attack (business continuity).

MSC Categories – Cybersecurity

Individual Accounts / Use of PWDS/Passphrases – 4.8 – Must

Implementation Guidance based on Recommendations from NIST

- Authentication: 2FA or MFA preferred
- Prefer the use of long easy to remember passphrases instead of passwords
- Require screening of new PWDS (commonly used/compromised PWDs)

MSC Categories – Cybersecurity

Backing up data / Confidential data encrypted – 4.12 – Should

Data backed up once a week / Facility offsite (cloud back up OK)

Store sensitive and confidential data in an encrypted format

Types: Cloud Storage; Internal Hard Disk Drive; Removable Storage Media

The 3-2-1 rule:

3 – Keep 3 copies of any important file: 1 primary and 2 backups

2 – Keep the files on 2 different media types

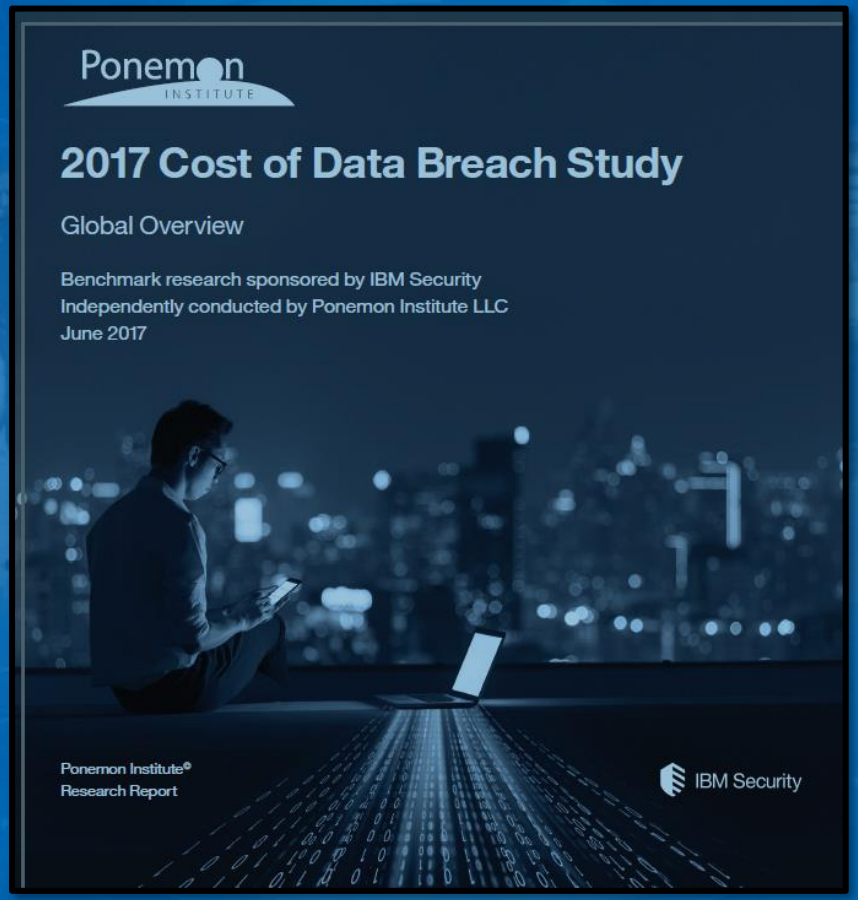
1- Store 1 copy offsite

MSC Categories – Cybersecurity

Ponemon Institute / IBM Study - 2017

- Average cost per data breach: $7.35 million USD
- Cost – Higher for malicious attacks (followed by system glitches and human error).
- Affects all industries – Average Cost per Record:

  Technology - $251
  Industrial - $259
  Transportation - $240



FireEye – 91% of all cyber crimes start with an e-mail. Training is critical!

MSC Categories – Agricultural Security

Agriculture is the largest business sector

⬇

Contaminants found in all conveyances

(all modes / all types of cargo - 352 pests discovered daily by CBP)

⬇

Contaminants harbor pests and diseases

⬇

Threaten this industry

⬇

We know that … and so do terrorists

⬇

Objective – Destroy our Economic Viability

New Category

Invasive species cause over $138B annually in economic and environmental losses. Eliminating contamination in conveyances and cargo may decrease holds, delays, and commodity returns and treatments.

MSC Categories – Agricultural Security

Insects & Snails	Plant Material & Seeds	Garbage & Organic Material
 Snails	 Cogon Grass	 Manure
 Grasshoppers	 Spilled seed on trailer floor	 Animal Blood
 Asian Gypsy moth egg masses	 Weed seeds stuck to WPM	 Soil Contamination
 Khapra Beetle Larvae	 Cottonseed in rail car springs	 Garbage contamination on rail

MSC Categories – Agricultural Security

New Category: Eliminating contaminants from the supply chain leads to decreases in CBP cargo holds, delays in cargo arriving at its destination, and the need for commodities to be re-exported or treated (fumigated).

Section 8 of the MSC – Only One Criterion – Core

Other MSC requirements related to AG security in other criteria categories.

•

8.1 – Written procedures to prevent pest contamination to include compliance with WPM Regulations.

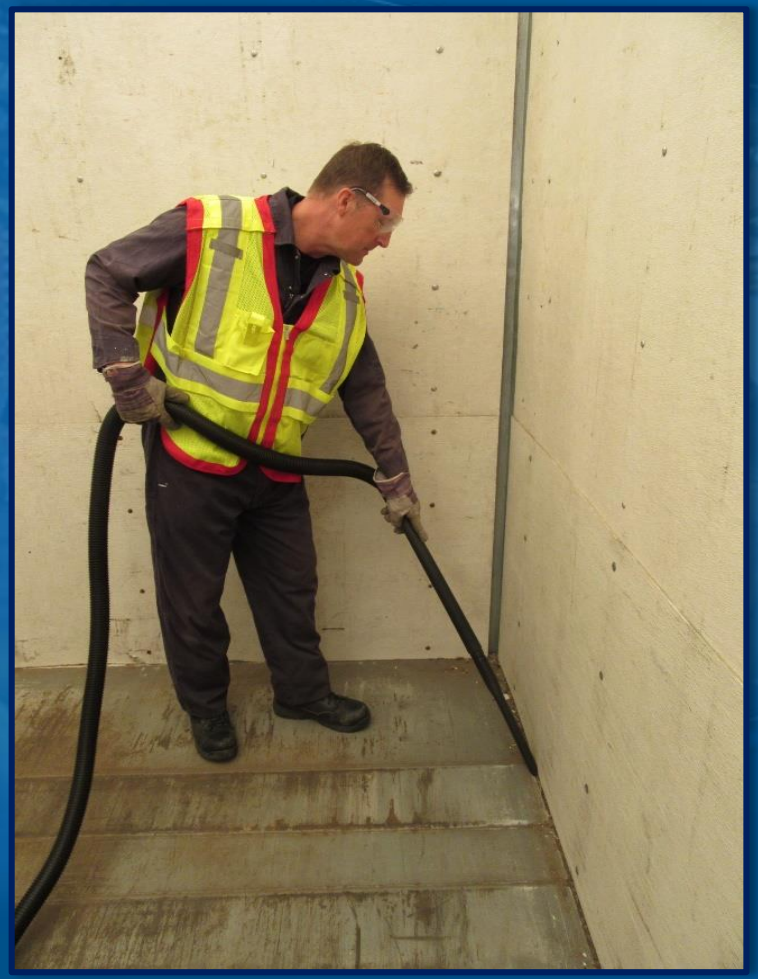
- All pest contamination
- IMO Definition of Pest Contamination: Visible
- WPM Highlighted

MSC Categories – Agricultural Security

Pest Contamination Definition – From International Maritime Organization

Pest contamination is defined as **visible** forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).“

MSC Categories – Agricultural Security



Eliminating Contaminants – Vacuum, Broom, Blower

MSC Categories – Agricultural Security

Start With Clean Container/Trailer Prior to Loading

Utilize Paved Lots to Avoid Contamination

MSC Categories – Business Partner Requirements / Forced Labor

New Topic: Eliminating forced labor practices from the supply chain.

- CTPAT Security – Included a Criterion As a Should or Recommendation

COAC Forced Labor and Trusted Trader Working Groups – On-going discussions on how the issue of forced labor will be incorporated into the CTPAT

MSC Categories – Business Partner Requirements / Forced Labor

CTPAT Members **should** have a documented social compliance program in place that, at a minimum, addresses how the company ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced, imprisoned, indentured, or indentured child labor.

Applicable Entities: Importers, Exporters, Foreign Manufacturers

Should – Recommendation – Bringing visibility to a serious issue

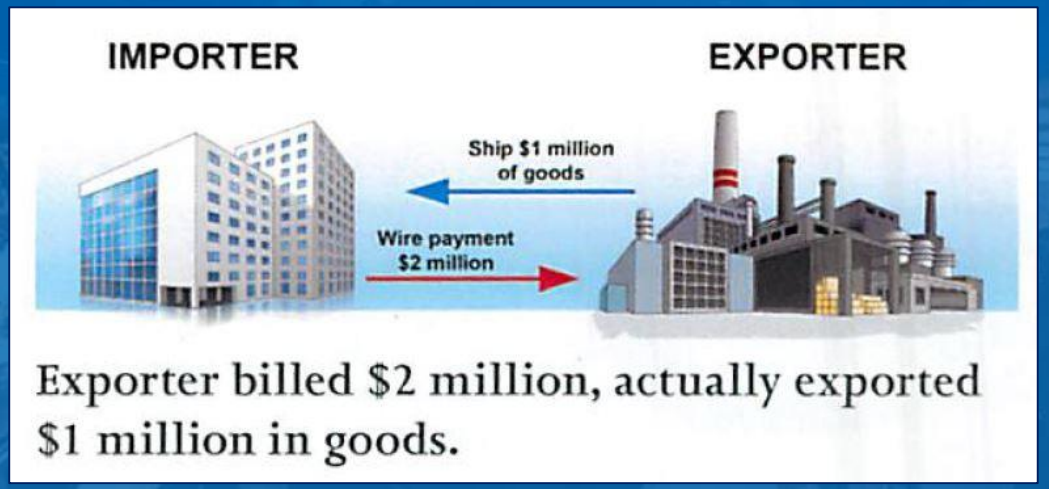
MSC Categories – Business Partner Requirements

New Topic: Combating money laundering and terrorist funding

CTPAT Members must have a written, risk based process for screening new business partners and for monitoring current partners. A factor that Members **should** include in this process is checks on activity related to money laundering and terrorist funding.

CTPAT Portal – Public Documents / Public Library

Warning Indicators of Trade Based Money Laundering and Terrorist Financing



Exporter billed $2 million, actually exported $1 million in goods.

Exporter billed $500K for silver, importer actually received $2 million of gold.

MSC – Other Criteria

- Recommend a no-stop policy for shipments in close proximity to the US.
- The inspection process for IIT, tractors and trailers as specified by CTPAT is now a requirement –not just a recommendation.
- Use of a checklist – remains a should but being more specific as to what should be on that checklist.
- Formally introducing the VVTT seal verification process to the MSC as a must.
- Transponders: carriers must either pay the annual user fee or the single crossing fee online prior to arrival at the POE.
- Transmit an electronic manifest for bobtails and empty containers prior to the arrival of the conveyance at the border.

MSC – Notifying/Reporting

- Carriers should notify appropriate parties of any significant delays during transit – 5.28
- Alert business partners of credible or detected threats – 5.29
- Must have written procedures for reporting an incident –including a escalation process – 7.23
- Should have a mechanism to report security related issues anonymously – 7.25

If you **see** something, **say** something®

1-800-BE ALERT (1-800-232-5378)
Hotline / Notify SCSS

MSC Categories – Physical Security / Security Technology

Should be utilized to monitor premises and prevent unauthorized access to sensitive areas – 9.7

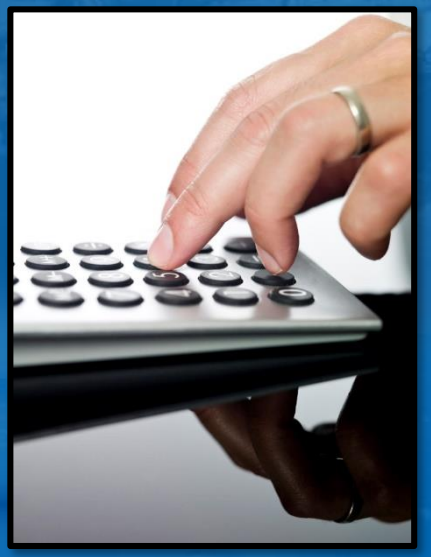
Security technology – Video surveillance systems such as closed circuit television cameras, intrusion alarms, access control devices, etc.

- Goal – make sure technology was set up properly; it is functioning well; it is being monitored; it is secured.
- Other AEO programs require the use of security technology
- Security technology – widely used. Example: SCAN: 7,300 audits in over 50 countries: only 219 factories did not have CCTV (3%) and they were issued corrective actions.
- The EU and GDPR – CCTV

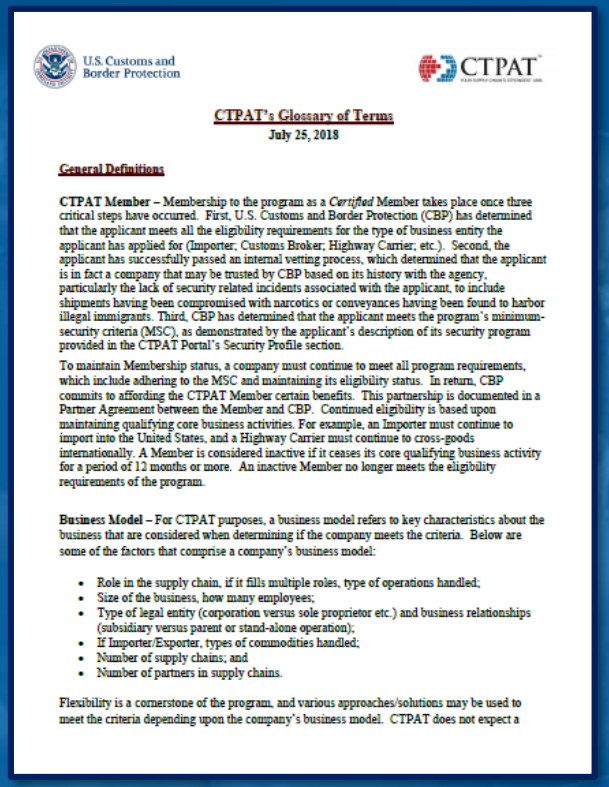
New Eligibility Requirements

New Eligibility Requirements – CORE

Maintain no evidence of financial debt to CBP for which the responsible party has exhausted all administrative and judicial remedies for relief, a final judgment or administrative disposition has been rendered, and the final bill or debt remains unpaid at the time of the initial application or annual renewal.



MSC Training Tools / Resources



U.S. Customs and Border Protection

CTPAT

CTPAT's Glossary of Terms

July 25, 2018

General Definitions

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

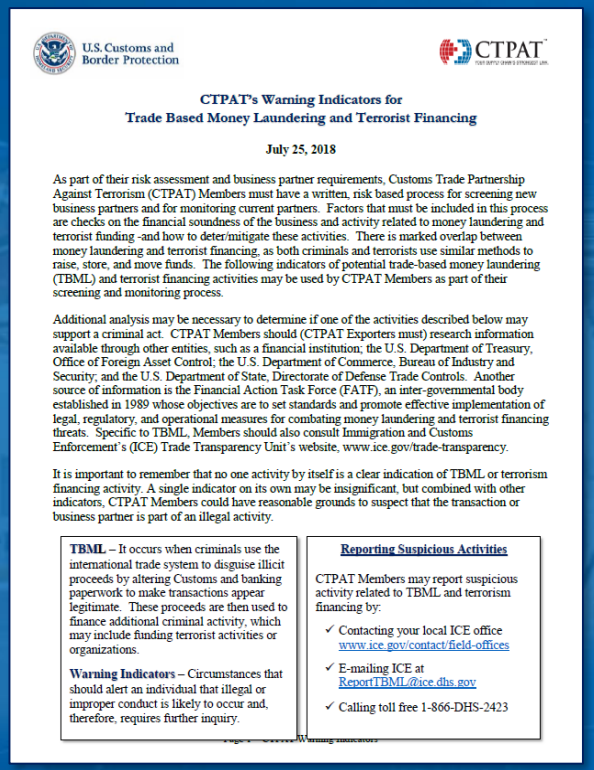
To maintain Membership status, a company must continue to meet all program requirements, which include adhering to the MSC and maintaining its eligibility status. In return, CBP commits to affording the CTPAT Member certain benefits. This partnership is documented in a Partner Agreement between the Member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

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

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

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

Glossary of Terms



U.S. Customs and Border Protection

CTPAT

CTPAT's Warning Indicators for Trade Based Money Laundering and Terrorist Financing

July 25, 2018

As part of their risk assessment and business partner requirements, Customs Trade Partnership Against Terrorism (CTPAT) Members must have a written, risk based process for screening new business partners and for monitoring current partners. Factors that must be included in this process are checks on the financial soundness of the business and activity related to money laundering and terrorist funding -and how to deter/mitigate these activities. There is marked overlap between money laundering and terrorist financing, as both criminals and terrorists use similar methods to raise, store, and move funds. The following indicators of potential trade-based money laundering (TBML) and terrorist financing activities may be used by CTPAT Members as part of their screening and monitoring process.

Additional analysis may be necessary to determine if one of the activities described below may support a criminal act. CTPAT Members should (CTPAT Exporters must) research information available through other entities, such as a financial institution; the U.S. Department of Treasury, Office of Foreign Asset Control; the U.S. Department of Commerce, Bureau of Industry and Security; and the U.S. Department of State, Directorate of Defense Trade Controls. Another source of information is the Financial Action Task Force (FATF), an inter-governmental body established in 1989 whose objectives are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering and terrorist financing threats. Specific to TBML, Members should also consult Immigration and Customs Enforcement's (ICE) Trade Transparency Unit's website, www.ice.gov/trade-transparency.

It is important to remember that no one activity by itself is a clear indication of TBML or terrorism financing activity. A single indicator on its own may be insignificant, but combined with other indicators, CTPAT Members could have reasonable grounds to suspect that the transaction or business partner is part of an illegal activity.

TBML – It occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

Warning Indicators – Circumstances that should alert an individual that illegal or improper conduct is likely to occur and, therefore, requires further inquiry.

Reporting Suspicious Activities

CTPAT Members may report suspicious activity related to TBML and terrorism financing by:

- ✓ Contacting your local ICE office www.ice.gov/contact/field-offices
- ✓ E-mailing ICE at ReportTBML@ice.dhs.gov
- ✓ Calling toll free 1-866-DHS-2423

Warning Indicators

U.S. Customs and Border Protection

Southern Border Truck Pest Contamination

Trade Outreach

U.S. Customs and Border Protection

May 2018

1

USDA

Agricultural Security

CTPAT Portal – Public Documents / Public Library

Next Steps – Timeline

May 2019 – MSC Booklets Released to Trade / CTPAT Portal: Public Documents: Public Library

One Booklet per Business Entity / Contain: MSC, Eligibility Requirements, and other important program information

Summer 2019: MSC Booklets uploaded to CTPAT website (Once they are 508 Compliant)

CTPAT Members - Implement Criteria in 2019

Validations on new Criteria – Begin in early 2020

Most Companies will NOT undergo a CTPAT Validation in 2020 - but ALL Companies Need to Implement and Comply.