GENERAL ASSOCIATE TRAINING FOR CTPAT’S SECURITY AND AWARENESS PROGRAM
Agenda

1. What is CTPAT
2. Background & Benefits
3. Leadership involvement
4. Keys to Partnership Success
5. Basic Supply Security Principles
6. Statement of Support
7. Key Reasons to Participate
8. What is Terrorism?
9. Why is this Training Important
10. Enterprise Responsibilities
11. Minimum Security Structure/Criteria
12. High Profile Concerns/Action to Take
13. Examples to Share
14. Changes for 202
15. Questions
16. Thank You
What is CTPAT?

- Customs Trade Partnership Against Terrorism (CTPAT) is but one layer in U.S. Customs and Border Protection’s (CBP) multi-layered cargo enforcement strategy.
- A program is U.S. Customs and Border Protection’s (CBP) premier trade security program.
- The purpose of CTPAT is to partner with the trade community for the purpose of securing the U.S. and international supply chains from possible intrusion by terrorist organizations.
- Requires the trade company participant to document and validate their supply chain security procedures in relation to existing CBP CTPAT criteria or guidelines as applicable.
- CBP requires that CTPAT company participants develop an internal validation process to ensure the existence of security measures documented in their supply chain Security Profile and in any supplemental information provided to CBP.
- As a part of the CTPAT process, CBP CTPAT Supply Chain Security Specialists (SCSS) and the CTPAT participant will jointly conduct a validation of the company’s supply chain security procedures. The validation process is essential to verifying the company’s commitment to CTPAT.

Background & Benefits

- **Background**
  - Reaction to 9/11/01 Attacks
  - Gore Enterprise involvement – MOU signed by Jim Buckley, 2003
  - US Customs national supply chain security partnership
  - Program has greater than 10,000 participants (Imports only)
  - Benchmark program for other global security supply chain initiatives
  - Third party relationships need to be considered
    - Suppliers & Freight forwarders
    - Couriers & Warehouses

- **Benefits**
  - Global Mutual Recognition (CTPAT and AEO)
  - Reduction in US Customs Inspections
  - Business Resumption
  - Front of the Line Privileges
CEO and Functional Leader Involvement

- Functions affected by the CTPAT portal requirements include:
  - Supply Chain, Security, Procurement, Human Resources, Information Technologies, Logistics, & Global Trade.

- Leaders are accountable for reviewing and updating CTPAT processes annually and are considered the Enterprise accountable representatives.

- The ‘Officer of the Enterprise’ reviews and submits all responses annually in the US Custom’s portal.
This illustrates the Minimum Security Requirements being supported by the accountable leadership. (Integrated senior leadership involvement is one of the new requirements.)

Expectations: As new requirements are initiated by Customs or Gore, procedures need to be updated in the portal integrating all the partners.
Manage Supply Chain Risk –

▪ Identify, assess, prioritize and assign roles to manage risk by utilizing a multi-layered approach of policy & procedures, clear function ownership and physical security solutions by subject matter experts.

▪ Ensures the policies and solutions are not only present but fit for purpose and effective. Qualified individuals to operate and inspect.

▪ Think big picture... Supply chain is global; program needs to be “end to end” worthy.... CBP thinks so as well!

▪ PLAN-DO-CHECK-ACT... is embedded in the “Trust but Verify concept!”
Basic Supply Chain Security Principles Continued

▪ “Know Before it Goes”... Especially if a regulated material arrives domestically

▪ Identify the Known Trusted Partners who will handle any part of the shipment; manufacturer-brokers-initial freight forwarder-consolidator-trucking/port/air and final domestic carrier from port of entry

▪ CBP is requiring near “real time” knowledge of where shipments of regulated materials coming into the USA are

▪ Determine if these Trusted Partners have been vetted by either their country equivalent Customs/Trade agencies or already have been vetted by CBP
Supply Chain Vision: Statement of Support

As a participant in CTPAT, Gore is making a firm commitment to enhance the security of goods moving through our international supply chain. Gore works to protect its supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. Allegations or indications of any of the above activities or risks in Gore's supply chain will be promptly investigated and appropriately addressed. An Associate who has evidence of or concerns about inappropriate or illegal conduct in Gore's supply chain are directed to contact their regional Trade team, their leader or the Gore's Ethics Hotline.

Signed://David Rurak
Key Reasons to Voluntarily Participate in CTPAT?

- Expedited release of the Enterprise’s cargo in destination ports within the United States during all threat levels designated by the Secretary
- Reduced cargo examinations
- Increased priority for cargo examinations
- Reduced penalties and lower risk score pursuant to the Automated Targeting System; and
- **Automatic mitigation to fines and penalties assessed against importers** - ASK!!
What is Terrorism?

- Terrorism is a defined set of actions and behaviors that attempt to cause:
  - Fear/panic
  - Disruption of services
  - Intimidation
  - Embarrassment to our leaders
  - Media attention
How To Identify Signs of Terrorism

▪ Terrorism is action and behavior – *it is not about physical appearance*

▪ Be aware of behaviors in the workplace like:
  - Someone recording or monitoring activity
  - Someone trying to access information they don’t need to have
  - Tests of security measures: physical barriers, security procedures, or electronic/digital security
  - Stealing of supplies, uniforms, or credentials
Why is This Training Important

- The threat of terrorism faces everyone, everywhere.
- The “global supply chain” & how it is a vulnerable target for terrorism.
- How to recognize a “possible” threat to security & safety, both in your workplace as well as other areas of the global supply chain.
- What to do if you suspect abnormal or unusual activity.
- Heighten participant awareness level of terrorism and both national and international security and terrorist threats.
- Enable participant to gain sufficient background on the issues of national security threats.

NOTE: This training is intended for the general Associate. If your commitment involves any of the functional areas within supply chain, please consult with your LEADER as additional training and knowledge may be required. (Supply Chain, Security, Procurement, Human Resources, Information Technologies, Logistics, Agricultural & Global Trade)
Overview of Enterprise’s Responsibilities

- Evaluates risks and threats to the Enterprise’s global supply chain, including the data infrastructure and documentation process.
- Provides re-current Security Training as changes occur or as situations warrant.
- Establish/Implement security policies, standards and procedures at the highest level of the company, as it pertains to security threats and security awareness.
- Choose vendors/service providers carefully, holding each vendor/service provider to the same security standards.
- Provide a clear mission of these critical policies to employees, business partners, customers and vendors...whether domestically or abroad.
- **Provides Security Threat Awareness Training to its Associates.**
# CTPAT MSC Structure

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

- **3 Focus Areas**
- **12 Security Criteria Categories**
- Each Criterion Has an ID Number
1. **Procedural Security**

   Security measures must be in place to ensure the integrity & security of processes relevant to the transportation, handling, & storage of cargo in the supply chain.

   - Controls for incoming & outgoing cargo
   - Receiving documentation, retention
   - Retention of import seals & corresponding documentation such as seal reports and receiving verification logs
   - Notification to law enforcement when breeches of security policy are detected

2. **Physical Security**

   Cargo handling & storage facilities, in domestic & foreign locations, must have physical barriers & deterrents that guard against unauthorized access.

   - Fencing/Lighting/Access Control
   - Video and video retention
   - Security monitoring/alarm systems
   - Assigned security management tasks and responsibilities to security members
   - Entry Identification policies
   - Exit inspections
3. Personnel Security

- Process must be in place to screen prospective employees & periodically check current employees.
- Applicant screening process
  - Criminal Background checks
  - Employment background checks
  - Removal of access

4. Education, Security Training & Threat Awareness

- A threat awareness program is established & maintained by the Enterprise to inform Associates to recognize & foster awareness of the threat posed by terrorists at each point in the supply chain.
  - Training for leadership, security members, & receivers
  - Education/awareness for all Associates
CTPAT Minimum Security Criteria

5. Site Access Control

- Access control prevents unauthorized and limited entry to facilities & limits access to Associates & visitors which protects Enterprise assets.
- Carriers – requirements for all deliveries (especially import containers)
- Delivery and pick up drivers must be limited to areas of restriction and not allowed in cargo storage areas through driver access controls

6. Container Manifest Verification

- Ensures the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately, timely, & exceptions documented.
- Receiving manifest verification process is mandatory to confirm shipment quantities and reporting of all shortages or overages
- Immediate investigation of shortages or overages upon discovery
- Reporting to CBP or law enforcement if not resolved internally
7. Container Security

- Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.
- Eight-point inspection
- Seal chain of custody
- No unauthorized access to containers
- **Agricultural** type inspections to ensure there is no signs or appearance of infestation or rodents at the point of container stuffing and unloading

8. IT Security

- Access restrictions – change password every 90 days & system locks after 3 failed attempts
- Monitoring Internet access
- Establishing & reviewing access levels
- Temporary access suspension – if an Associate is on leave, access temporary suspended
- Virus/firewall/tampering prevention – virus detection, data encryption, & virus quarantine
- Data back-up & recovery – contingency plan to protect IT systems
- Hardware security – controlling work station access, password screen saver, & securing server
9. Corporate Responsibility

- The demonstration of senior management endorsement of CTPAT security execution of MSC
- Leadership involvement with global security enhanced awareness for the company
- Financial commitment to implementation of elevated security controls
- Demonstration of support for internal CTPAT security committee through divisional and business unit boundaries

10. Cyber Security

- The demonstration of commitment to prevent hacking and unauthorized access to company automated systems
- Written and verifiable SOP’s that demonstrate the existence of Cyber Security controls in place for US and global company personnel with systems access
- Schedule and routine system testing to ensure cyber security controls are operational and functional capturing attempts of unauthorized access.
High Profiled Functional Concerns & Actions to Take

Specialized training should be provided to Associates whose commitment involves or has the potential for the following:

- Procurement and accounting – know the warning indicators of Trade Based Money Laundering and Terrorism Financing
- Business and Logistics - Supply chain freight at rest is freight at risk (need to track)
- Facilities and Logistics – Agricultural requirements to include pest control measures
- Support teams - Mail Rooms
- Security - Reporting CTPAT and security incidents (example: unauthorized “person”, non/incorrectly badged personnel in unauthorized areas)
- Receivers and inventory control – Reporting overages and shortages

### Actions to take:

<table>
<thead>
<tr>
<th>W.L. Gore &amp; Associate Locations</th>
<th>Internal</th>
<th>External Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Eastern Cluster</td>
<td>60000</td>
<td>410-506-0000</td>
<td><a href="mailto:security@wlgore.com">security@wlgore.com</a></td>
</tr>
<tr>
<td>U.S. Western Cluster - FLG</td>
<td>43610</td>
<td>928-864-3610</td>
<td><a href="mailto:westernussecurity@wlgore.com">westernussecurity@wlgore.com</a></td>
</tr>
<tr>
<td>U.S. Western Cluster - PHS</td>
<td>45610</td>
<td>623-234-5610</td>
<td><a href="mailto:westernussecurity@wlgore.com">westernussecurity@wlgore.com</a></td>
</tr>
</tbody>
</table>
Examples of Global Supply Chain Suspicious Activities

- Suspicious types of mail/boxes not matching the post marked location.
- Items received that are not noted on the packing slip, bill of lading, work order or other documentation pertaining to this shipment, this could be suspicious and should be investigated.
Yard Lighting & Fence Line Procedures

- Security team monitors yard lighting ensuring area is adequately covered for safety & security line maintained with 4 - 6' clear line of sight on both sides.

- Security reports issues to Facilities team for repair when needed.

- Security team monitors trailer yards to ensure no unauthorized access by anyone including visitors, non-authorized contractors or drivers.

- Advanced notice, if visitor or contractor granted access to location.

- Any exceptions challenged by security team & immediately reported.
CTPAT as it moves into 2020

- Moving from voluntary to mandatory compliance
- Adds new compliance requirements
- Strengthens current requirements
- Increases the number of Customs on-site physical inspections that determines if a site meets “validation” requirements
- Ensures the Enterprise has “end to end” supply chain security measures in place

Demonstration of security controls are essential to the retention of the Enterprise’s CTPAT good standing.
CTPAT in 2020

▪ Terrorism personally affects every individual.

▪ Security, police and the military cannot be “everywhere.” We all must do our share in this effort of global security.

▪ Heightened awareness communicates confidence. We are not “easy targets.” This increases our chance of preventing a serious incident.

▪ **STAY ALERT, if you see something, contact Security.**

<table>
<thead>
<tr>
<th>W.L. Gore &amp; Asso. Locations</th>
<th>Internal</th>
<th>External Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Eastern Cluster</td>
<td>60000</td>
<td>410-506-0000</td>
<td>security@wl Gore.com</td>
</tr>
<tr>
<td>U.S. Western Cluster - FLG</td>
<td>43610</td>
<td>928-864-3610</td>
<td>westernussecurity@wl Gore.com</td>
</tr>
<tr>
<td>U.S. Western Cluster - PHS</td>
<td>45610</td>
<td>623-234-5610</td>
<td>westernussecurity@wl Gore.com</td>
</tr>
</tbody>
</table>

▪ Security will notify the CTPAT team via the security communication protocol.

▪ CTPAT questions, email to: [CTPAT@WLGORE.com](mailto:CTPAT@WLGORE.com) or call Gary Cooke @ 410 506 2839.
THANK YOU