TO: International Suppliers shipping to the United States

PPG Industries, Inc., and its affiliates have been certified as a member of the U. S. Customs Trade Partnership Against Terrorism ("C-TPAT"). C-TPAT is a U. S. government-business initiative launched to strengthen supply chain security. As part of the ongoing process, PPG must assess its own security practices as well as communicate Customs C-TPAT security recommendations to international business partners to encourage review and enhancement of their security processes as needed. In addition, PPG must ensure that new U.S. Customs mandatory supply chain security requirements are being met.

What we need from you:

- **If your company is involved with international shipments to PPG in the U.S. including returned goods or packaging,** refer this letter to the security representative most knowledgeable about shipments to PPG.

- **Read the attached supply chain security recommendations and new U. S. Customs mandatory supply chain security requirements concerning international container seals, physical security and access controls.**

- Return the attached PPG Supply Chain Security Acknowledgement by email, fax, or mail within two weeks from receipt.

- U. S. Customs could request an on-site visit to your facility to verify that the new C-TPAT security requirements have been met. Accessibility to written security procedures and evidence of periodic review of internal controls to ensure compliance will be beneficial.

Adherence to C-TPAT security recommendations will help strengthen security for all supply chain members. Questions about C-TPAT may be directed to Jasmin Lussier, Chief Compliance Officer at 412-434-3200 or by email to jlussier@ppg.com. Foreign manufacturers can now apply for membership in the C-TPAT program. In order to strengthen our partnership, PPG encourages your participation. Further information about C-TPAT is available at the U.S. Customs website: http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

I appreciate your cooperation in this important security initiative.

PPG Supply Chain Security Acknowledgement

Read the attached C-TPAT security recommendations from U. S. Customs. Then describe your company's security procedures related to exports to PPG in the U.S. by checking (√) the appropriate blocks below.

Select (√) the category that best describes your business with PPG entities in the U. S.

	Manufacturer
	Warehouse Operator
	Customer returning U.S. originating products, packing materials, etc.
	Other, specify type

What PPG location(s) in the United States does your company most frequently ship to?

	Comments

Does your company have written security procedures at non-U.S. facilities doing business with PPG and conduct periodic reviews of internal controls to ensure security compliance?

	Yes
	No
	Comments

Does your company affix seals to loaded containers for shipments to PPG in the U.S.?

	Yes, *specify type*
	No
	Comments

Please note that as of May 15, 2014, U.S. Customs requires that all containers in transit to the United States are required to be sealed with a seal meeting the ISO/PAS 17712:2013 standard. Please see ISO 17712:2013 Bulletin for more information.

Does your company store containers?

	Yes
	No
	Comments

If yes to the above question, are containers in a secure area to prevent unauthorized access or manipulation?

	Yes
	No
	Comments

Does your company have procedures in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors? (See the following link for items to be addressed during a container inspection: Inspection Procedure)**?**

	Yes
	No
	Comments

Does your company have physical access controls to prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets?

	Yes
	No
	Comments

Have you developed and communicated a process to report shipment overages/shortages, losses or abnormalities, whether suspected or confirmed, to PPG management?

	Yes
	No
	Comments

Has your company been accepted by U.S. Customs as a certified member of C-TPAT, the Business Anti-Smuggling Coalition (BASC) or other internationally-recognized security initiatives?

	Yes, C-TPAT, **Specify SVI#**
	Yes, FAST
	Yes, BASC
	Yes, specify other
	No
	Comments

Identify the individual to whom questions about security of PPG shipments may be directed:

Contact Name & Title		Phone	
Company Name		Email	
Address		Fax	

(insert Company Name) _____ acknowledges PPG's emphasis on supply chain security and recognizes the expectation that business partners share that commitment. I understand that PPG may refer security inquiries from U. S. Customs to me.

NAME: _____TITLE_____

SIGNATURE: _____ DATE _____

Minimum Security Criteria for C-TPAT

These minimum security criteria are fundamentally designed to be the building blocks for foreign manufacturers to institute effective security practices designed to optimize supply chain performance to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain. The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies, and in particular, foreign manufacturers to elevate their security practices.

At a minimum, on a yearly basis, or as circumstances dictate such as during periods of heightened alert, security breach or incident, foreign manufacturers must conduct a comprehensive assessment of their international supply chains based upon the following C-TPAT security criteria. Where a foreign manufacturer out-sources or contracts elements of their supply chain, such as another foreign facility, warehouse, or other elements, the foreign manufacturer must work with these business partners to ensure that 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 (manufacturer/supplier/vendor) through to point of distribution – and recognizes the diverse business models C-TPAT members employ.

C-TPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk[1]. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model.

Appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the Foreign manufacturer's supply chains - based on risk[2].

Business Partner Requirement
Foreign manufacturers must have written and verifiable processes for the selection of business partners including, carriers, other manufacturers, product suppliers and vendors (parts and raw material suppliers, etc).

Security procedures
For those business partners eligible for C-TPAT certification (carriers, importers, ports, terminals, brokers, consolidators, etc.) the foreign manufacturer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified.

For those business partners not eligible for C-TPAT certification, the foreign manufacturer must require that their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., contractual obligations; via a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent World Customs Organization (WCO) accredited security program administered by a foreign customs authority; or, by providing a completed foreign manufacturer security questionnaire). Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the foreign manufacturer.

Point of Origin
Foreign manufacturers must ensure that business partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of origin, assembly or manufacturing. Periodic reviews of business partners' processes and

facilities should be conducted based on risk, and should maintain the security standards required by the foreign manufacturer.

Participation/Certification in a Foreign Customs Administration Supply Chain Security Program
Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the foreign manufacturer.

Security Procedures
On U.S. bound shipments, foreign manufacturers should monitor that C-TPAT carriers that subcontract transportation services to other carriers use other C-TPAT approved carriers, or non-C-TPAT carriers that are meeting the C-TPAT security criteria as outlined in the business partner requirements.

As the foreign manufacturer is responsible for loading trailers and containers, they should work with the carrier to provide reassurance that there are effective security procedures and controls implemented at the point-of-stuffing.

Container and Trailer Security
Container and trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers and trailers. A high security seal must be affixed to all loaded containers and trailers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standard for high security seals.

In those geographic areas where risk assessments warrant checking containers or trailers for human concealment or smuggling, such procedures should be designed to address this risk at the manufacturing facility or point-of-stuffing.

Container Inspection
Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

Trailer Inspection
Procedures must be in place to verify the physical integrity of the trailer structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. The following ten-point inspection process is recommended for all trailers:

- Fifth wheel area - check natural compartment/skid plate
- Exterior - front/sides
- Rear - bumper/doors
- Front wall
- Left side
- Right side

- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

Container and Trailer Seals
The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of a foreign manufacturers' commitment to C-TPAT. The foreign manufacturer must affix a high security seal to all loaded trailers and containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers and trailers, to include procedures for recognizing and reporting compromised seals and/or containers/trailers to US Customs and Border Protection or the appropriate foreign authority. Only designated employees should distribute seals for integrity purposes.

Container and Trailer Storage
Containers and trailers under foreign manufacturer control or located in a facility of the foreign manufacturer must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

Physical Access Controls
Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

Employees
An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

Visitors
Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and should visibly display temporary identification.

Deliveries (including mail)
Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated.

Challenging and Removing Unauthorized Persons
Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Personnel Security
Processes must be in place to screen prospective employees and to periodically check current employees.

Pre-Employment Verification
Application information, such as employment history and references must be verified prior to employment.

Background Checks / Investigations
Consistent with foreign regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

Personnel Termination Procedures
Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

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

Documentation Processing
Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

Manifesting Procedures
To help ensure the integrity of cargo, procedures must be in place to ensure that information received from business partners is reported accurately and timely.

Shipping and Receiving
Departing cargo being shipped should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Procedures should also be established to track the timely movement of incoming and outgoing goods.

Cargo Discrepancies
All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies must be notified if anomalies, illegal or suspicious activities are detected - as appropriate.

Physical Security
Cargo handling and storage facilities in international locations must have physical barriers and deterrents that guard against unauthorized access. Foreign manufacturer should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

Fencing
Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.

Gates and Gate Houses
Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

Parking
Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

Building Structure
Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

Locking Devices and Key Controls
All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

Lighting
Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

Alarms Systems and Video Surveillance Cameras
Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Information Technology Security
Password Protection
Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

Accountability
A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.

Security Training and Threat Awareness
A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists and contraband smugglers at each point in the supply chain. Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.

Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

[1] Foreign manufacturers shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, C-TPAT membership, potential terrorist threat via open source information, having inadequate security, past security incidents, etc.).

[2] Foreign manufacturer shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, potential terrorist threat via open source information, etc.))