C-TPAT VALIDATION PROCESS GUIDELINES

I. Introduction

The Customs Service has developed a validation process to ensure that C-TPAT participants have implemented the security measures outlined in their Security Profile and in any supplemental information provided to Customs. The validation process will be conducted jointly by U.S. Customs personnel and a representative of the industry participant. The validation will focus on the material in the participant's C-TPAT security profile and any related materials provided by the participant and will be conducted under the guiding partnership principles of C-TPAT.

II. Objective

The purpose of the validation is to ensure that the supply chain security measures contained in the C-TPAT participant's security profile have been implemented and are being followed. In the context of the company's operations and the C-TPAT security recommendations, the validation team will evaluate the status and effectiveness of key security measures in the participant's profile and make recommendations where appropriate.

III. Validation Principles

The guiding principle of the C-TPAT program is partnership. The C-TPAT program is voluntary and designed to share information that will protect the supply chain from being compromised by terrorists and terrorist organizations.

The validation process will enable Customs and the C-TPAT participant to jointly review the participant's C-TPAT security profile to ensure that security actions in the profile are being effectively executed. Throughout the process there will also be the opportunity to discuss security issues and to share "best practices" with the ultimate goal of securing the international supply chain.

C-TPAT validations are not audits. In addition, they will be focused, concise, and will last not longer than ten work days.

Based on the participant's C-TPAT security profile and the recommendations of the validation team, Headquarters will also oversee the specific security elements to be validated.

IV. Conducting a Validation

A. Validation Selection Process

To ensure their accuracy, the security profiles of C-TPAT participants will be validated. The order in which a C-TPAT participant's profile will be selected for validation will be based on risk management principles. Validations may be initiated based on import volume, security related anomalies, strategic threat posed by geographic regions, or other risk related information. Alternatively, a validation may be performed as a matter of routine program oversight. Customs Headquarters will schedule a company's first validation within approximately three years of the company becoming a C-TPAT certified participant. Customs field offices will not initiate validations and unannounced validations will not be conducted. C-TPAT participants will be given thirty days advance written notice along with a request for any supporting documentation that is needed.

B. Partnership Validation Teams

A Partnership Validation Team (PVT), consisting of Customs Office of Field Operations personnel and a representative of the C-TPAT participant, will conduct the on-site C-TPAT validation.

Customs representatives on a PVT will be officers knowledgeable in supply chain security matters. Customs PVT members will receive supply chain security training to assist them in working with industry representatives to promote effective corporate supply chain security programs. Customs Headquarters will determine the Customs representatives for each PVT. All Customs PVT representatives will be personnel from the Office of Field Operations.

The Customs Partnership Validation Team Leader (assigned by Customs Headquarters) will be responsible for the team's reviewing the company's security profile, other security information provided by the company, and data and information retrievable from other sources to determine the focus of the validation. This will help ensure that the validation is effective and limited in duration.

C. Validation Venue

A validation is an on-site review of the participant's C-TPAT supply chain security profile. The actual site of the validation may vary depending on the aspect(s) of the participant's profile that the "C-TPAT Validation Team" will review.

Under normal circumstances the validation will begin with a briefing of company officials at the domestic corporate office or facility of the C-TPAT participant. If additional data or information is required to validate a portion of a C-TPAT

participant's supply chain domestically or overseas, the PVT leader will request approval of travel through the Director, C-TPAT, at Customs Headquarters.

D. Validation Procedures

Upon receiving direction from Headquarters, Customs PVT leader will provide the company with a written notification of the scheduled validation. The notice will be issued at least thirty days prior to the start of the validation and will include a request for supporting documentation or materials, if any. The PVT leader will also contact the C-TPAT participant to establish a single point of contact at the corporate level.

Each validation will be customized for the participant involved and focused on the company's C-TPAT security profile. Prior to the on-site validation, the Customs representatives on the PVT will review the participant's C-TPAT security profile, any supplemental information received from the company, and any Customs Headquarters instructions, to determine the extent and focus of the validation.

In preparation for the on-site validation, the validation team may also consider pertinent C-TPAT security recommendations. A complete set of recommendations is included as Attachment A below. These security recommendations are a reference tool for considering the sufficiency of specific aspects of a participant's C-TPAT security profile. It is understood that the recommendations are not mandatory and are not all-inclusive with respect to effective security practices.

As noted earlier, to begin the validation, the PVT will meet with company officials to discuss the process. Upon completion of the validation, the PVT will again convene with company officers to discuss validation findings. Although not a part of the PVT, the company's Customs account manager will normally attend the company briefings that initiate and complete the validation process.

E. Validation Report

Validation findings will be documented, included in the team's final report, and forwarded to the Director of C-TPAT for final editing and sharing with the C-TPAT participant. Ideally the report will affirm or increase the level of benefits provided to the participant. However, depending on the findings, some or all of the participant's C-TPAT benefits may be deferred until corrective action is taken to address identified vulnerabilities. With respect to actions resulting from a validation, Customs authority will rest with the Executive Director, Border Security and Facilitation.

ATTACHMENT A

PREFACE

The following outlines the C-TPAT Security Recommendations that may be used by the C-TPAT Validation Team in the planning phase of an on-site validation. The recommendations are not mandatory for C-TPAT participation, but they may be helpful in the pre-validation review of key aspects of a participant's C-TPAT security profile. Therefore, prior to conducting an on-site validation, the validation team may review and discuss appropriate security recommendations contained in these attachments in the context of the participant's C-TPAT security profile. This will assist the team in limiting the scope of the validation and in customizing the validation to the C-TPAT participant involved.

IMPORTERS

Develop and implement a sound plan to enhance security procedures throughout your supply chain. Where an importer does not control a facility, conveyance or process subject to these recommendations, the importer agrees to make every reasonable effort to secure compliance by the responsible party. The following are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

Procedural Security: Procedures should be in place to protect against unmanifested material being introduced into the supply chain. Security controls should include the supervised introduction/removal of cargo, the proper marking, weighing, counting and documenting of cargo/cargo equipment verified against manifest documents, the detecting/reporting of shortages/overages, and procedures for verifying seals on containers, trailers, and railcars. The movement of incoming/outgoing goods should be monitored. Random, unannounced security assessments of areas in your company's control within the supply chain should be conducted. Procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company should also be in place.

Physical Security: All buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include perimeter fences, locking devices on external and internal doors, windows, gates and fences, adequate lighting inside and outside the facility, and the segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

Access Controls: Unauthorized access to facilities and conveyances should be prohibited. Controls should include positive identification all employees, visitors, and vendors. Procedures should also include challenging unauthorized/unidentified persons.

Personnel Security: Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

Education and Training Awareness: A security awareness program should be provided to employees including the recognition of internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should offer incentives for active employee participation in security controls.

Manifest Procedures: Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

Conveyance Security: Conveyance integrity should be maintained to protect against the introduction of unauthorized personnel and material. Security should include the physical search of all readily accessible areas, the securing of internal/external compartments and panels, and procedures for reporting cases in which unauthorized personnel, unmanifested materials, or signs of tampering, are discovered.

BROKERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

Procedural Security: Companies should notify Customs and other law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

Documentation Processing: Brokers should make their best efforts to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information. Documentation controls should include, where applicable, procedures for:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.
- Recording, reporting, and/or investigating shortages and overages of merchandise/cargo.
- Safeguarding computer access and information.

Personnel Security: Consistent with federal, state, and local regulations and statutes, companies should establish an internal process to screen prospective employees, and verify employment applications. Such an internal process could include background checks and other tests depending on the particular employee function involved.

Education and Training Awareness: A security awareness program should include notification being provided to Customs and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected. These programs should provide:

- Recognition for active employee participation in security controls.
- Training in documentation fraud and computer security controls.

MANUFACTURERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case by case basis depending on the company's size and structure and may not be applicable to all. The company should have a written security procedure plan in place that addresses the following:

Physical Security: All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates, and fences.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.

Access Controls: Unauthorized access to the shipping, loading dock and cargo areas should be prohibited. Controls should include:

- The positive identification of all employees, visitors and vendors.
- Procedures for challenging unauthorized/unidentified persons.

Procedural Security: Measures for the handling of incoming and outgoing goods should include the protection against the introduction, exchange, or loss of any legal or illegal material. Security controls should include:

- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented products.
- Procedures for verifying seals on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures for tracking the timely movement of incoming and outgoing goods.
- Proper storage of empty and full containers to prevent unauthorized access.
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

Personnel Security: Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

Education and Training Awareness: A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining product integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

WAREHOUSES

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all. Warehouses as defined in this guideline are facilities that are used to store and stage both Customs bonded and non-bonded cargo. The company should have a written security procedure plan in place addressing the following:

Physical Security: All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates and fences.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.

Access Controls: Unauthorized access to facilities should be prohibited. Controls should include:

- The positive identification of all employees, visitors, and vendors.
- Procedures for challenging unauthorized/unidentified persons.

Procedural Security: Procedures should be in place to protect against unmanifested material being introduced into the warehouse. Security controls should include:

- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented cargo/cargo equipment verified against manifest documents.
- Procedures for verifying seal on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.
- Proper storage of empty and full containers to prevent unauthorized access.

Personnel Security: Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

Education and Training Awareness: A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

AIR CARRIERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

Conveyance Security: Aircraft integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical search of all readily accessible areas, securing all internal/external compartments and panels, and reporting cases in which unmanifested materials, or signs of tampering, are discovered.

Access Controls: Unauthorized access to the aircraft should be prohibited. Controls should include the positive identification of all employees, visitors and vendors as well as procedures for challenging unauthorized/unidentified persons.

Procedural Security: Procedures should be in place to protect against unmanifested material being introduced aboard the aircraft. Security controls should include complete, accurate and advanced lists of international passengers, crews, and cargo, as well as a positive baggage match identification system providing for the constant security of all baggage. All cargo/cargo equipment should be properly marked, weighed, counted, and documented under the supervision of a designated security officer. There should be procedures for recording, reporting, and/or investigating shortages and overages, and procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the carrier.

Manifest Procedures: Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

Personnel Security: Employment screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted.

Education and Training Awareness: A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

Physical Security: Carrier's buildings, warehouses, and on & off ramp facilities should be constructed of materials which resist unlawful entry and protect against outside intrusion. Physical security should include adequate locking devices for external and internal doors, windows, gates and fences. Perimeter fencing should also be provided, as well as adequate lighting inside and outside the facility; including parking areas. There should also be segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by means of a safe, cage, or otherwise fenced-in area.

SEA CARRIERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

Conveyance Security: Vessel integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security should include the physical search of all readily accessible areas, the securing all internal/external compartments and panels as appropriate, and procedures for reporting cases in which unmanifested materials, or signs of tampering, are discovered.

Access Controls: Unauthorized access to the vessel should be prohibited. Controls should include the positive identification of all employees, visitors, and vendors. Procedures for challenging unauthorized/unidentified persons should be in place.

Procedural Security: Procedures should be in place to protect against unmanifested material being introduced aboard the vessel. Security procedures should provide for complete, accurate and advanced lists of crews and passengers. Cargo should be loaded and discharged in a secure manner under supervision of a designated security representative and shortages/overages should be reported appropriately. There should also be procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company.

Manifest Procedures: Manifests should be complete, legible, accurate and submitted in a timely manner pursuant to Customs regulations.

Personnel Security: Employment screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted.

Education and Training Awareness: A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

Physical Security: Carrier's buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include adequate perimeter fencing, lighting inside and outside the facility, and locking devices on external and internal doors, windows, gates, and fences.

LAND CARRIERS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

Conveyance Security: Integrity should be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical search of all readily accessible areas, securing all internal/external compartments and panels, and procedures for reporting cases in which unmanifested materials, or signs of tampering, are discovered.

Physical Security: All carrier buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include adequate locking devices on external and internal doors, windows, gates and fences. Perimeter fencing should be addressed, as well as adequate lighting inside and outside the facility, to include the parking areas. There should be segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

Access Controls: Unauthorized access to facilities and conveyances should be prohibited. Controls should include the positive identification of all employees, visitors, and vendors as well as procedures for challenging unauthorized/unidentified persons.

Procedural Security: Procedures should be in place to protect against unmanifested material being introduced aboard the conveyance. Security controls should include the proper marking, weighing, counting, and documenting of cargo/cargo equipment under the supervision of a designated security representative. Procedures should be in place for verifying seals on containers, trailers, and railcars, and a system for detecting and reporting shortages and overages. The timely movement of incoming and outgoing goods should be tracked and there should be procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

Manifest Procedures: Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

Personnel Security: Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications.

Education and Training Awareness: A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

AIR FREIGHT CONSOLIDATORS/ OCEAN TRANSPORTATION INTERMEDIARIES, AND NVOCCS

Develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company's size and structure and may not be applicable to all.

Procedural Security: Companies should notify Customs and other law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

Documentation Processing: Consolidators should make their best efforts to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information. Documentation controls should include, where applicable, procedures for:

- Maintaining the accuracy of information received, including the shipper and consignee name and address, first and second notify parties, description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.
- Recording, reporting, and/or investigating shortages and overages of merchandise/cargo.
- Tracking the movement of incoming and outgoing cargo.
- Safeguarding computer access and information.

Companies should participate in the Automated Manifested System (AMS) and all data submissions should be complete, legible, accurate and submitted in a timely manner pursuant to Customs regulations.

Personnel Security: Consistent with federal, state, and local regulations and statutes, companies should establish an internal process to screen prospective employees, and verify applications. Such an internal process could include background checks and other tests depending on the particular employee function involved.

Education and Training Awareness: A security awareness program should include notification being provided to Customs and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected. These programs should provide:

- Recognition for active employee participation in security controls.
- Training in documentation fraud and computer security controls.