



U. S. Customs Service

Customs-Trade Partnership Against Terrorism



June 20, 2003

C-TPAT Guide



Strategic Solutions Partners, LLC

Table of Contents

Description of Contents	3
Importer Security Recommendations for C-TPAT	7
Importer Instructions for C-TPAT	8
Required Documentation: Importer - C-TPAT Agreement to Voluntarily Participate	10
Required Documentation: Importers - C-TPAT Supply Chain Security Profile Questionnaire	12
Licensed Customs Broker	13
Licensed Customs Broker Instructions for C-TPAT	13
Licensed Customs Broker - Security Recommendations for C-TPAT	15
Required Documentation: Licensed Customs Broker - C-TPAT Supply Chain Security Profile Questionnaire	16
Licensed Customs Broker - C-TPAT Agreement to Voluntarily Participate	17
Third Party Consolidators	19
Air Freight Consolidators, Ocean Transportation Intermediaries and NVOCCs Security Recommendations for C-TPAT	19
Air Freight Consolidators/Ocean Transportation Intermediaries, and NVOCCs - Instructions for C-TPAT	20
Required Documentation: Air Freight Consolidators, Ocean Transportation Intermediaries and Non-Vessel Operating Carriers – C-TPAT Agreement to Voluntarily Participate	22
Required Documentation: Brokers, Air Freight Consolidators, Ocean Transportation Intermediaries and NVOCCs - C-TPAT Supply Chain Security Profile Questionnaire	24
C-TPAT Frequently Asked Questions - Air Freight Consolidators, Ocean Transportation Intermediaries, Brokers and NVOCCs	25
Carriers	26
Air Carrier	26
Air Carrier Security Recommendations for C-TPAT	26
Air Carrier Instructions for C-TPAT	27
Instructions:	27
Required Documentation: Air Carrier - C-TPAT Agreement to Voluntarily Participate	29
Specifically, the Carrier agrees to:	29
Specifically, Customs agrees to:	30
Sea Carrier	32
Sea Carrier Security Recommendations for C-TPAT	32
Sea Carrier Instructions for C-TPAT	33
Required Documentation: Sea Carrier - C-TPAT Agreement to Voluntarily Participate	35
Required Documentation: Sea Carrier - C-TPAT Supply Chain Security Profile Questionnaire	39
Rail Carrier	40
Rail Carrier Security Recommendations for C-TPAT	40
Rail Carrier Instructions for C-TPAT	41
Required Documentation: Rail Carrier - C-TPAT Agreement to Voluntarily Participate	43
Required Documentation: Rail Carrier - C-TPAT Supply Chain Security Profile Questionnaire	46
C-TPAT Frequently Asked Questions - Air, Rail, and Sea Carriers	47
U.S. Marine Ports and Terminals	49
U.S. Marine Port/Terminal Security Recommendations for Customs Trade Partnership Against Terrorism (C-TPAT)	49

U.S. Marine Port/Terminal Application Instructions for Customs-Trade Partnership Against Terrorism	51
U.S. Marine Port Authority/Terminal Operator Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism	53
U.S. Marine Port Authority/Terminal Operator Security Profile Questionnaire	56
Warehouse Security Recommendations.....	57
Manufacturer Security Recommendations	58

Description of Contents

The purpose of this document is to give as complete a document as possible describing the participation and requirements of **Customs-Trade Partnership Against Terrorism (C-TPAT)**.

Specifically, the document is segregated by application, i.e., importers, brokers, third parties, carriers, and port and terminal facilities.

Within each section are: recommendations, instructions for completing the C-TPAT agreement, and a supply-chain, security profile questionnaire.

Specific reference may also be obtained from the U.S. Customs website
http://www.customs.ustrreas.gov/xp/cgov/import/commercial_enforcement/ctpat/.

Alan Davis

Strategic Solutions Partners

June 20, 2003



C-TPAT Fact Sheet and Frequently Asked Questions

What is C-TPAT?

- C-TPAT is a joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security.
- C-TPAT recognizes that Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain, importers, carriers, brokers, warehouse operators, and manufacturers.
- Through this initiative, Customs is asking businesses to ensure the integrity of their security practices and communicate their security guidelines to their business partners within the supply chain.

What does participation in C-TPAT require?

Businesses must apply to participate in C-TPAT. Participants will sign an agreement that commits them to the following actions:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community. These guidelines, which are available for review on the Customs website, encompass the following areas: Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, and Conveyance Security.
- Submit a supply-chain, security profile questionnaire to Customs.
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

What are the benefits of participation in C-TPAT?

C-TPAT offers businesses an opportunity to play an active role in the war against terrorism. By participating in this first worldwide supply chain security initiative, companies will ensure a more secure supply chain for their employees, suppliers and customers. Beyond these essential security benefits, Customs will offer potential benefits to C-TPAT members, including:

- A reduced number of inspections (reduced border times)
- An assigned account manager (if one is not already assigned)
- Access to the C-TPAT membership list
- Eligibility for account-based processes (bimonthly/monthly payments, e. g.)
- An emphasis on self-policing, not Customs verifications

Who is eligible for C-TPAT?

C-TPAT is currently open to all importers and carriers (air, rail, sea). Customs plans to open enrollment to a broader spectrum of the trade community in the near future. C-TPAT membership will be made available to all sectors of the supply chain. Customs will be consulting with the trade community to develop the most effective approach for each sector to participate in

C-TPAT. Please refer to this site for the latest information on eligibility and application procedures.

How do I apply?

- Applicants will submit signed agreements to Customs, which will represent their commitment to the C-TPAT security guidelines.
- Applicants will also submit a supply-chain, security profile questionnaire at the same time they submit their signed agreements or within a specified time thereafter.
- Complete application instructions will be maintained on this site.

When will benefits begin?

Benefits will begin once Customs has completed an evaluation of the importer's C-TPAT application package and notified the importer of our findings. Customs aims to complete these evaluations within 30-60 days after the supply-chain, security questionnaire has been submitted.

How will the partnership work on an ongoing basis?

- Account managers will contact participants to begin joint work on establishing or updating account action plans to reflect C-TPAT commitments.
- Action plans will track participants' progress in making security improvements, communicating C-TPAT guidelines to business partners, and establishing improved security relationships with other companies.
- Failure to meet C-TPAT commitments will result in suspension of C-TPAT benefits. Benefits will be reinstated upon correcting identified deficiencies in compliance and/or security.
-

Where can I get more information on C-TPAT?

C-TPAT information will be maintained on this site.

Frequently Asked Questions

Q: What exactly are Customs expectations for the trade on this program?

A: To make a commitment toward the common goal of creating a more secure and efficient supply chain through partnership. Customs understands that it has entered a new era and requires the assistance of private industry to ensure increased vigilance throughout the supply chain. Customs recognizes that just as it protects the trade and our borders, businesses must ensure that their brands, employees, and customers are protected to the best of their abilities.

Q: Will the information our company provides be confidential?

A: All information on supply chain security submitted by companies applying for the C-TPAT program will be confidential. Customs will not disclose a company's participation in C-TPAT without the company's consent.

Q: As a company, we are very interested in C-TPAT but we are not interested in spending a lot of money, nor putting ourselves in a liability position if something goes wrong. Is it still possible to do this partnership?

A: Yes. Customs intent is to not impose security requirements that will be cost prohibitive. For this reason, we worked in concert with the trade community in developing security guidelines that reflect a realistic business perspective. Potential C-TPAT participants may find that they already have many of these guidelines in place.

C-TPAT is also not intended to create any new 'liabilities' for companies beyond existing trade laws and regulations. However, joining C-TPAT will commit companies to follow through on actions specified in the signed agreement. These actions include self-assessing security systems,

submitting security questionnaires, developing security enhancement plans, and communicating C-TPAT guidelines to companies in the supply chain. If a company fails to uphold its C-TPAT commitments, Customs would take action to suspend benefits or cancel participation.

Q: What is the overall vision for C-TPAT in the coming months and years?

A: Customs recognizes that a safe and secure supply chain is the most critical part of our work in keeping our country safe. For this reason, Customs is seeking a strong anti-terrorism partnership with the trade community through C-TPAT. Trade partners will have a commitment to both trade security and trade compliance, which are rooted in the same business practices. Customs wants to work closely with companies whose good business practices ensure supply chain security and compliance with trade laws.

Q: How will audits work in the future?

A: Audits will continue to be used to assess overall trade compliance. Customs Regulatory Audit will apply the new “Focused Assessment” methodology, a risk-based audit program, in conducting these audits. Companies will not be required to undergo a Focused Assessment in order to participate in C-TPAT. However, to take advantage of Customs Regulatory Audit Importer Self-Assessment (ISA) program, importers must be C-TPAT participants.

Q: As a carrier, I already participate in the Customs Carrier Initiative - is it a duplication of effort in joining C-TPAT?

A: Customs will be looking for carriers to join C-TPAT to enhance existing security practices and better address the terrorism threat to international air, sea, and land shipping. We will work to ensure that C-TPAT participation does not require duplicate work for current Customs Carrier Initiative Program (CIP) participants. CIP participants already subscribe to the importance of security from a narcotics-smuggling perspective and are well positioned to expand their security focus to encompass anti-terrorism.

Q: Is the C-TPAT program a viable consideration for medium or small size companies?

A: C-TPAT is designed for the entire trade community and Customs encourages all companies to take an active role in promoting supply chain and border security. While the benefits of C-TPAT are greatest for large companies that rely heavily on international supply chains, C-TPAT is not just a big-company program. Medium and small companies may want to evaluate the requirements and benefits of C-TPAT carefully in deciding whether to apply for the program. Moreover, even without official participation in C-TPAT, companies should still consider employing C-TPAT guidelines in their security practices.

For More Information:

Contact Industry Partnership Programs at (202) 927-0520 or email, at industry.partnership@customs.treas.gov



Importer Security Recommendations for C-TPAT

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 un-manifested 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, un-manifested materials, or signs of tampering, are discovered.



Importer Instructions for C-TPAT

Effective April 17, 2002, membership in the Customs-Trade Partnership Against Terrorism (C-TPAT) is open to all importers and carriers (air, rail, sea). To apply for participation in the C-TPAT, follow the Application Instructions. Complete the Agreement to Voluntarily Participate and the Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT Fact Sheet is available on the website to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions please contact U.S. Customs Industry Partnership Programs at industry.partnership@customs.treas.gov

Instructions:

1. Review and sign the “Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism.” This represents the applicant’s commitment to the C-TPAT security recommendations and the applicant’s commitment to work with its service providers throughout its supply chain to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.
2. Return two original signed Agreements to:
**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**
3. Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:
 - a. Official Company Name
 - b. Street Address, including zip code
 - c. Company Point of Contact to include:
 - Name of Point of Contact and title
 - Telephone Number
 - Fax Number
 - E-mail Address
4. Complete the Supply-chain, security profile questionnaire and:

- a. Mail an electronic copy contained on a 3.5” floppy disk or a CD-ROM to the address listed in item number 2.
 - Or
 - b. E-mail a copy to industry.partnership@customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire”
5. The following guidance is provided to better inform you on how to complete the Supply Chain Security Profile Questionnaire:
- a. The focus of the profile should be on the Importers Supply Chain, including the foreign countries you operate in and/or conduct business.
 - b. The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes and confirm that they have an active security program in place.
NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to Customs as part of the profile response.
 - c. Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti Smuggling Coalition (BASC).
 - d. Note the specific importing entities, identified by the importer number (IRS number), which are covered by the security process you detail. Specify the relationship of the listed importing entities to the company making application.
6. Upon receipt Customs will review, the importers completed Supply Chain Security Profile Questionnaire. After Customs completes it’s review the importer will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on their application within 60 days.
7. An electronic confirmation indicating receipt of a signed agreement will be sent to the e-mail address provided in the application.



Required Documentation: Importer - C-TPAT Agreement to Voluntarily Participate

This Agreement is made between _____, of _____ USA (hereafter referred to as “the Importer”) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Importer and Customs is intended to enhance the joint efforts of the Importer and Customs to develop a more secure border environment by focusing on the physical security of the production, transportation, and importation elements of the supply chain process. Customs and the Importer recognize the need to address these security issues in order to maintain an efficient and compliant import process.

The Importer agrees to develop and implement, within a framework consistent with the attached recommendations/guidelines, a verifiable, documented program to enhance security procedures throughout its supply chain process. Where the importer does not exercise control of a production facility, transportation or distribution entity, or process in the supply chain, the importer agrees to communicate the attached recommendations/guidelines to its suppliers and transportation/distribution service providers and, where practical, condition its relationships to those entities on the acceptance and implementation of the attached recommendations/guidelines.

Specifically, the Importer agrees to:

1. Sign and return this agreement to the U.S. Customs Service, Office of Field Operations, Industry Partnership Programs.
2. Complete and return the attached Supply-chain, security profile questionnaire within 60 days of signing and returning the agreement to Customs. Upon request from the importer, an extension, not to exceed 30 days, may be granted to complete the security questionnaire.
3. Companies will be asked to implement security and/or trade compliance improvement programs, included in their account action plans, when applicable.

Specifically, Customs agrees to:

1. Provide feedback and recommendations to the Importer on the information provided in the Supply-chain, security profile questionnaire within 60 days of receipt. Provide technical guidance when requested and when practical.
2. Consider the Importer’s acceptance and implementation of the listed guidelines when making risk determinations for the purposes of cargo examinations and document reviews.

The listed recommendations/guidelines reflect the mutual understanding of the Importer and Customs of what constitutes the basic elements of supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Importer.

This Agreement is subject to review by the Importer or Customs and may be terminated with written notice by either party.

This Agreement cannot, by law, exempt the Importer from any statutory or regulatory sanctions in the event that discrepancies are discovered during a physical examination of cargo or the review of documents associated with the Importer's Customs transactions.

All information provided by the Importer to Customs pursuant to this Agreement will remain confidential. Customs will not disclose the Importer's identity as a C-TPAT participant without the Importer's consent.

Nothing in this Agreement relieves the Importer of any responsibilities with respect to United States law, including the Customs Regulations.

Assistant Commissioner
Office of Field Operations
United States Customs Service

Name & Title
Company



Required Documentation: Importers - C-TPAT Supply Chain Security Profile Questionnaire

1.) Provide an executive summary outlining the process elements of the security procedures you currently have in place. Your submission must include the importer of record number(s), which are covered by the security processes you describe. At minimum, address the following elements:

- Security Program:
 1. Facilities security.
 2. Theft prevention.
 3. Shipping and receiving controls.
 4. Information security controls - integrity of automated systems.
 5. Internal controls - process established for reporting and correcting problems.
- Personnel Security:
 6. Pre-employment screening & periodic background reviews.
 7. Employee training on security awareness and procedures.
 8. Internal codes of conduct.
 9. Internal controls - process established for reporting and managing problems related to personnel security.
- Service Provider Requirements - Product suppliers, Carriers, Forwarders:
 10. Written standards for service providers' physical plant security.
 11. Quality controls on production processes to ensure system integrity.
 12. Financial assessment process to determine service provider's fiscal soundness and ability to deliver goods and services within contract parameters.
 13. Internal controls for the selection of service providers.
 14. Profiles of Tier 1 suppliers (i.e. those entities receiving and packing a finished commodity, for transportation to the final destination) maintained and available for review.
 15. Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti-Smuggling Coalition (BASC).

2.) Indicate that the specific detailed procedures noted above are available to Customs in a verifiable format at an identified location.

- Include an assessment of your security processes, as well as information on what changes you envision making to correct identified weaknesses.

Note: Identifying perceived weaknesses will not necessarily prohibit participation in C-TPAT. Customs is committed to working with you to identify effective corrections and adjustments to your processes that will result in a more secure supply chain operation. We have specific programs in place that can assist your company in meeting this objective. Our Carrier Initiative Program Coordinators can provide expert advice on establishing security programs throughout your supply chain. Program information will be provided upon request.



Licensed Customs Broker

Licensed Customs Broker Instructions for C-TPAT

To apply for participation in the C-TPAT, follow the instructions noted below to complete the Broker/Freight Forwarder/NVOCC Application to Voluntarily Participate and the Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT “Fact Sheet” is available to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions please contact U.S. Customs Industry Partnership Programs, at industry.partnership@customs.treas.gov

Instructions

1. Review and sign the “Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism.” This represents the applicant’s commitment to C-TPAT security recommendations and the applicant’s commitment to work with its service providers and customers throughout its supply chain to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.
2. Return two original signed Agreements to:
**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**
3. Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:
 - a. Official Company Name
 - b. Street Address, including zip code
 - c. Company Point of Contact to include:
 - Name of Point of Contact and title
 - Telephone Number
 - Fax Number
 - E-mail Address
4. Complete the Supply-chain, security profile questionnaire and additionally:
 - a. Mail an electronic copy contained on a 3.5” floppy disk or a CD-ROM to the address listed in item number 2.

OR

- b. E-mail a copy to industry.partnership@customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire”.
5. The following guidance is provided to better inform you on how to complete the Supply Chain Security Profile Questionnaire:
 - a. The focus of the profile should be on the operations your company performs, including the foreign countries you operate in and/or conduct business.
 - b. The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes and confirm that they have an active security program in place.

NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to Customs as part of the profile response.
 - c. Indicate if your service providers participate in Customs Industry Partnership Programs: Customs-Trade Partnership Against Terrorism (C-TPAT), Carrier Initiative Program (CIP), Super Carrier Initiative Program (SCIP), Business Anti-Smuggling Coalition (BASC).
6. Upon receipt, Customs will review the completed Supply Chain Security Profile Questionnaire. After Customs completes its review, the company will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on its application within 60 days.
7. An electronic confirmation indicating receipt of a signed agreement will be sent to the e-mail address provided in the application.



Licensed Customs Broker - Security Recommendations for C-TPAT

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.



Required Documentation: Licensed Customs Broker - C-TPAT Supply Chain Security Profile Questionnaire

1.) Provide an executive summary outlining the process elements of the security procedures you currently have in place and which are relevant to your operation/function. At minimum, address the following elements:

- Security Program:
 1. Facilities security.
 2. Theft prevention.
 3. Shipping and receiving controls.
 4. Information security controls - integrity of automated systems.
 5. Internal controls - process established for reporting and correcting problems.

- Personnel Security:
 6. Pre-employment screening & periodic background reviews.
 7. Employee training on security awareness and procedures.
 8. Internal codes of conduct.
 9. Internal controls - process established for reporting and managing problems related to personnel security.

- Service Provider Requirements (i.e., Contract Security Companies):
 10. Written standards for service providers' physical and procedural security.
 11. Internal controls for the selection of service providers.
 12. Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti-Smuggling Coalition (BASC).

2.) Indicate that the specific detailed procedures noted above are available to Customs in a verifiable format at an identified location.

- Include an assessment of your security processes, as well as information on what changes you envision making to improve security. Identifying perceived weaknesses or gaps will not necessarily prohibit participation in C-TPAT. Customs is committed to working with you to identify effective corrections and adjustments to your processes that will result in a more secure supply chain operation. We have specific programs in place that can assist your company in meeting this objective. Our Industry Partnership Program Coordinators can provide expert advice on establishing security programs throughout your supply chain. Program information will be provided upon request.



Licensed Customs Broker - C-TPAT Agreement to Voluntarily Participate

This Agreement is made between _____, of _____ USA (hereafter referred to as “the Broker”) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Broker and Customs is intended to enhance the joint efforts of the Broker and Customs to develop a more secure border environment by focusing on the accuracy and timeliness of information provided to Customs during the cargo entry and clearance process, by increasing the awareness of brokerage employees and clients on the importance of supply chain security, and by exchanging relevant information when security-related discrepancies are detected. Customs and the Broker recognize the need to address these security issues in order to maintain an efficient and compliant import process.

The Broker agrees to develop and implement, within a framework consistent with the listed recommendations/guidelines, a verifiable, documented program to enhance security procedures and increase security awareness throughout its operations. The broker agrees to communicate the attached recommendations and guidelines to its clients during the normal course of business.

Specifically, the Broker agrees to:

1. Sign and return this agreement to the U.S. Customs Service, Office of Field Operations.
2. Complete and return the attached Security Profile Questionnaire within 60 days of signing and returning the agreement to Customs. An additional 30 days may be granted upon request.
3. Brokers will be asked to implement security and/or trade compliance improvement programs, included in their account action plans, when needed.

Specifically, Customs agrees to:

1. Provide feedback and recommendations to the Broker on the information provided in the Security Profile Questionnaire within 30 days of receipt.
2. Provide technical guidance when requested and when practical.
3. Consider the Broker’s acceptance and implementation of the listed guidelines when making risk determinations for the purposes of cargo examinations and document reviews.

The listed recommendations/guidelines reflect the mutual understanding of the Broker and Customs of what constitutes the basic elements of supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Broker.

This Agreement is subject to review by the Broker or Customs and may be terminated with written notice by either party.

This Agreement cannot, by law, exempt the Broker from any statutory or regulatory sanctions associated with the Broker’s responsibilities in its Customs transactions.

Nothing in this Agreement relieves the Broker of any responsibilities with respect to United States law, including the Customs Regulations.

Name & Title
United States Customs

Name & Title
Service Company



Third Party Consolidators

Air Freight Consolidators, Ocean Transportation Intermediaries and NVOCCs Security Recommendations for C-TPAT

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.



Air Freight Consolidators/Ocean Transportation Intermediaries, and NVOCCs - Instructions for C-TPAT

To apply for participation in the C-TPAT, follow the instructions noted below to complete the Broker/Freight Forwarder/NVOCC Application to Voluntarily Participate and the Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT “Fact Sheet” is available to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions please contact U.S. Customs Industry Partnership Programs, at industry.partnership@customs.treas.gov

Instructions

Review and sign the “Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism.” This represents the applicant’s commitment to C-TPAT security recommendations and the applicant’s commitment to work with its service providers and customers throughout its supply chain to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.

Return two original signed Agreements to:

**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**

Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:

Official Company Name
Street Address, including zip code
Company Point of Contact to include:

- Name of Point of Contact and title
- Telephone Number
- Fax Number
- E-mail Address
-

Complete the Supply-chain, security profile questionnaire and additionally:

Mail an electronic copy contained on a 3.5” floppy disk or a CD-ROM to the address listed in item number 2.

OR

E-mail a copy to industry.partnership@customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire.”

The following guidance is provided to better inform you on how to complete the Supply Chain Security Profile Questionnaire:

The focus of the profile should be on the operations your company performs, including the foreign countries you operate in and/or conduct business.

The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes and confirm that they have an active security program in place.

NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to Customs as part of the profile response.

Indicate if your service providers participate in Customs Industry Partnership Programs: Customs-Trade Partnership Against Terrorism (C-TPAT), Carrier Initiative Program (CIP), Super Carrier Initiative Program (SCIP), Business Anti-Smuggling Coalition (BASC).

Upon receipt, Customs will review the completed Supply Chain Security Profile Questionnaire. After Customs completes its review, the company will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on its application within 60 days.

An electronic confirmation indicating receipt of a signed agreement will be sent to the e-mail address provided in the application.



Required Documentation: Air Freight Consolidators, Ocean Transportation Intermediaries and Non-Vessel Operating Carriers – C-TPAT Agreement to Voluntarily Participate

This Agreement is made between _____, of _____ USA (hereafter referred to as “the Consolidator”) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Consolidator and Customs is intended to enhance the joint efforts of the Consolidator and Customs to develop a more secure border environment by focusing on the accuracy and timeliness of information provided to Customs during the cargo entry and clearance process, by increasing the awareness of the Consolidator’s employees and clients on the importance of supply chain security, and by exchanging relevant information when security-related discrepancies are detected. Customs and the Consolidator recognize the need to address these security issues in order to maintain an efficient and compliant import process.

The Consolidator agrees to develop and implement, within a framework consistent with the listed recommendations/guidelines, a verifiable, documented program to enhance security procedures and increase security awareness throughout its operations. The Consolidator agrees to communicate the attached recommendations and guidelines to its clients during the normal course of business.

Specifically, the Consolidator agrees to:

1. Sign and return this agreement to the U.S. Customs Service, Office of Field Operations.
2. Complete and return the attached Security Profile Questionnaire within 60 days of signing and returning the agreement to Customs. An additional 30 days may be granted upon request.
3. Consolidators will be asked to implement security and/or compliance improvement programs, when needed.

Specifically, Customs agrees to:

1. Provide feedback and recommendations to the Consolidator on the information provided in the Security Profile Questionnaire within 30 days of receipt.
2. Provide technical guidance when requested and when practical.
3. Consider the Consolidator’s acceptance and implementation of the listed guidelines when making risk determinations for the purposes of cargo examinations and document reviews.

The listed recommendations/guidelines reflect the mutual understanding of the Consolidator and Customs of what constitutes the basic elements of supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Consolidator.

This Agreement is subject to review by the Consolidator or Customs and may be terminated with written notice by either party.

This Agreement cannot, by law, exempt the Consolidator from any statutory or regulatory sanctions in the event that discrepancies are discovered during a physical examination of cargo or the review of documents associated with the Consolidator's Customs transactions.

Nothing in this Agreement relieves the Consolidator of any responsibilities with respect to United States law, including the Customs Regulations.

Name & Title
United States Customs

Name & Title
Service Company



Required Documentation: Brokers, Air Freight Consolidators, Ocean Transportation Intermediaries and NVOCCs - C-TPAT Supply Chain Security Profile Questionnaire

1.) Provide an executive summary outlining the process elements of the security procedures you currently have in place and which are relevant to your operation/function. At minimum, address the following elements:

- Security Program:
 1. Facilities security.
 2. Theft prevention.
 3. Shipping and receiving controls.
 4. Information security controls - integrity of automated systems.
 5. Internal controls - process established for reporting and correcting problems.

- Personnel Security:
 1. Pre-employment screening & periodic background reviews.
 2. Employee training on security awareness and procedures.
 3. Internal codes of conduct.
 4. Internal controls - process established for reporting and managing problems related to personnel security.

- Service Provider Requirements (i.e., Contract Security Companies):
 1. Written standards for service providers' physical and procedural security.
 2. Internal controls for the selection of service providers.
 3. Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti-Smuggling Coalition (BASC).

2.) Indicate that the specific detailed procedures noted above are available to Customs in a verifiable format at an identified location.

- Include an assessment of your security processes, as well as information on what changes you envision making to improve security. Identifying perceived weaknesses or gaps will not necessarily prohibit participation in C-TPAT. Customs is committed to working with you to identify effective corrections and adjustments to your processes that will result in a more secure supply chain operation. We have specific programs in place that can assist your company in meeting this objective. Our Industry Partnership Program Coordinators can provide expert advice on establishing security programs throughout your supply chain. Program information will be provided upon request.



C-TPAT Frequently Asked Questions - Air Freight Consolidators, Ocean Transportation Intermediaries, Brokers and NVOCCs

Q: Is C-TPAT a voluntary program for brokers, airfreight consolidators/ocean transportation intermediaries, and NVOCCs?

A: Yes. C-TPAT is designed to build upon existing relationships with the various sectors of the trade community to enlist voluntary participation in the program to develop and enhance relevant security practices.

Q: Should our company sign more than one agreement if we perform multiple functions (e.g. brokerage and freight forwarding)?

A: Yes. Sign the agreements that pertain to the functions you perform and note on the security profile submission that your company does perform multiple services and that you agree to the appropriate security recommendations for that service function.

Q: Will we be designated as a broker account when we sign onto C-TPAT?

A: Account status is one of the potential benefits of C-TPAT participation. Account status designation will be determined based on a variety of factors, including C-TPAT participation.

Q: Will freight forwarders/consolidators and NVOCCs be designated as accounts when they sign onto C-TPAT?

A: As the initiative evolves, account status may be extended to forwarders and NVOCCs as a potential benefit.

Q: Are there monetary penalties associated with C-TPAT?

A: No.

Q: Will brokers be required to do background checks on all their employees?

A: No. However, it is expected that pre-employment verification will be done on all new hires and that a more detailed background review will be completed when significant issues arise.

For more Information:

Contact the Industry Partnership Programs, at (202) 927-0520 or email, at industry.partnership@customs.treas.gov



Carriers

Air Carrier

Air Carrier Security Recommendations for C-TPAT

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 un-manifested 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 un-manifested 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.



Air Carrier Instructions for C-TPAT

To apply for participation in the C-TPAT, follow the instructions noted below to complete the Air Carrier Application to Voluntarily Participate and the Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT “Fact Sheet” is available to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions please contact U.S. Customs Industry Partnership Programs at industry.partnership@customs.treas.gov

Instructions:

1. Review and sign the “Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism.” This represents the applicant’s commitment to the C-TPAT security recommendations and the applicant’s commitment to work with its service providers throughout its supply chain to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.
2. Return two original signed Agreements to:
**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**
3. Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:
 - a. Official Company Name
 - b. Street Address, including zip code
 - c. Company Point of Contact to include:
 - Name of Point of Contact and title
 - Telephone Number
 - Fax Number
 - E-mail Address
4. Complete the Supply-chain, security profile questionnaire and additionally:
 - Mail an electronic copy contained on a 3.5” floppy disk or a CD-ROM to the address listed in item number 2.

Or

E-mail a copy to industry.partnership@customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire”

5. The following guidance is provided to better inform you on how to complete the Supply Chain Security Profile Questionnaire:

- a. The focus of the profile should be on the Carrier's Supply Chain, including the foreign countries you operate in and/or conduct business.
- b. The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes and confirm that they have an active security program in place.

NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to Customs as part of the profile response.

- c. Indicate if your service providers participate in Customs Industry Partnership Programs: Customs-Trade Partnership Against Terrorism (C-TPAT), Carrier Initiative Program (CIP), Super Carrier Initiative Program (SCIP), Business Anti-Smuggling Coalition (BASC).

Upon receipt, Customs will review the carrier's completed Supply Chain Security Profile Questionnaire. After Customs completes its review, the carrier will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on its application within 60 days.

An electronic confirmation indicating receipt of a signed agreement will be sent to the e-mail address provided in the application.



Required Documentation: Air Carrier - C-TPAT Agreement to Voluntarily Participate

This Agreement is made between _____, of _____ (hereafter referred to as “the Carrier”) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Carrier and Customs is intended to enhance the joint efforts of both entities in developing a more secure border environment by improving the security for the transportation of passengers, crew, conveyances and cargo throughout the commercial process. Customs and the Carrier recognize the need to improve and expand existing security practices in order to achieve a more efficient and compliant import process.

The Carrier agrees to develop and implement, within a framework consistent with the listed recommendations, a verifiable, documented program to enhance security procedures throughout its supply chain process. Where the Carrier does not exercise control of a production facility, distribution entity, or process in the supply chain, the Carrier agrees to communicate the attached recommendations/guidelines to those entities.

Specifically, the Carrier agrees to:

1. Complete and return the attached Air Carrier Supply-chain, security profile questionnaire within 60 days of signing and returning the agreement to Customs. Upon request from the carrier, an extension, not to exceed 30 days, may be granted to complete the security questionnaire.
2. Immediately before departure to the United States, conduct a comprehensive aircraft search by means of a checklist or other mutually acceptable method.
3. Ensure the integrity of all compartments and panels.
4. Ensure that only authorized personnel displaying proper identification can obtain access to its aircraft, both abroad and in the United States.
5. Credentialing and background checks of employees will be conducted as required by appropriate federal and state statutes and regulations.
6. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to Customs upon written request, to the extent permitted by law.
7. Implement a Positive Baggage Identification Match (PBIM) program. The Carrier’s SOP will describe in detail a plan to ensure that all checked baggage has an accompanying passenger checked in and boarded onto the aircraft.
8. Maintain constant control of all baggage from the check-in point to the aircraft, and from the aircraft to the Customs baggage examination area.
9. Provide security at the carrier’s cargo warehouse facility.
10. Ensure that all air waybills and other documentation submitted for cargo is complete and a system in place to verify the accuracy of the weight, marks and quantity of the cargo received for shipment.

11. Notify Customs promptly of the existence of manifest discrepancies.
12. Participate with Customs in joint security surveys at selected facilities both abroad and in the U.S.
13. Designate, at each U.S. port of entry, the carrier official or representative who will serve as the primary liaison with Customs at that port.
14. Participate in the Advanced Passenger Information System (APIS) and the air Automated Manifest System (AMS).
15. Promptly provide to Customs, upon request, all available flight information on specific passengers/cargo.
16. Notify Customs of irregular cargo shipments/shippers.
17. Require, as a matter of Carrier policy, that all employees cooperate fully with Customs in implementing the various actions and initiatives of this Agreement.
18. Conduct periodic unannounced security checks to ensure that all procedures are being performed in accordance with defined guidelines.
19. A security awareness program should be developed and 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.
20. Ensure contract companies that provide carrier related services establish and adhere to carrier security standards. Periodically review contract services for possible weaknesses in security.
21. Provide Customs, upon request, with documentation that demonstrates compliance with each item of this agreement.
22. To the extent possible and where feasible, cooperate with U.S. Customs, domestic and foreign port authorities, foreign customs administrations, and other industry leaders, in advancing the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI).

Specifically, Customs agrees to:

1. Acknowledge that the prime responsibility of the Carrier lies in the safe and expeditious movement of cargo and the facilitation, to the greatest extent possible, of the Carrier's legitimate business concerns, not that of a law enforcement agency.
2. Consider the Carrier's acceptance and implementation of the listed guidelines when making risk determinations for the purposes of cargo examinations and document reviews.
3. Review the Carrier's application package and provide feedback and recommendations to the Carrier on the information provided in the Air Carrier Supply-chain, security profile questionnaire within 60 days of receipt.
4. Conduct initial and periodic conveyance, facility and procedural surveys. All surveys will include a report from Customs on its findings and recommendations for improvements.

5. Participate with the carrier in developing a security awareness program.
6. Will not request that the Carrier takes any action, which will conflict with the laws, regulations, or control requirements of any country.
7. Assist the Carrier in identifying high-risk ports, routes, and facilities, and in assessing its vulnerability to terrorism.
8. Participate with the Carrier in joint security surveys at the selected facilities both abroad and in the United States.
9. In addition to an Account Manager, Customs will provide a point of contact at each United States port served by the Carrier for all matters relative to this Agreement.
10. Coordinate with Carrier management press releases or information to the public, which directly involve the Carrier's interest. The joint and cooperative nature of this Agreement will be emphasized.

Distribute to carrier C-TPAT participants cleared information regarding

The listed Security Recommendations reflect the mutual understanding of the Carrier and Customs of what constitutes the basic elements of the carrier's supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Carrier. The Carrier's security profile, submitted pursuant to this agreement, and incorporated as part of the jointly developed plan, represents the Carrier's and Customs acknowledgement and understanding of the terms of this Agreement.

This Agreement is subject to review by the Carrier or Customs and may be terminated with written notice by either party.

This Agreement cannot, by law, exempt the Carrier from any statutory or regulatory sanctions in the event that discrepancies are discovered during a physical examination of cargo or the review of documents associated with the Carrier Customs transactions.

Nothing in this Agreement relieves the Carrier of any responsibilities with respect to United States law, including the Customs Regulations.

Name & Title
United States Customs

Name & Title
Service Company



Sea Carrier

Sea Carrier Security Recommendations for C-TPAT

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 un-manifested 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 un-manifested 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.



Sea Carrier Instructions for C-TPAT

To apply for participation in the C-TPAT, follow the instructions noted below to complete the Sea Carrier Agreement to Voluntarily Participate and the Carrier Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT "Fact Sheet" is available to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions please contact U.S. Customs Industry Partnership Programs at industry.partnership@customs.treas.gov

Instructions:

Review and sign the "Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism." This represents the applicant's commitment to the C-TPAT security recommendations and the applicant's commitment to work with its service providers to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.

Return two original signed Agreements to:

**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**

Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:

2. Official Company Name
3. Street Address, including zip code
4. Company Point of Contact to include:
 - Name of Point of Contact and title
 - Telephone Number
 - Fax Number
 - E-mail Address
 -

Complete the Carrier Supply-chain, security profile questionnaire and additionally:

Mail an electronic copy contained on a 3.5" floppy disk or a CD-ROM to the address listed in item number 2.

Or

E-mail a copy to industry.partnership@customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire.”

The following guidance is provided to better inform you on how to complete the Carrier Supply Chain Security Profile Questionnaire:

The focus of the profile should be on the Carrier operations, including the foreign countries you operate in and/or conduct business.

The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes (e.g., contract security companies) and confirm that they have an active security program in place.

NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to U.S. Customs as part of the profile response.

Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti Smuggling Coalition (BASC).

Upon receipt, Customs will review the carrier’s completed Carrier Supply Chain Security Profile Questionnaire. After Customs completes its review, the carrier will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on its application within 60 days.

An electronic confirmation indicating receipt of a signed agreement will be sent to the e-mail address provided in the application.



Required Documentation: Sea Carrier - C-TPAT Agreement to Voluntarily Participate

This Agreement is made between _____, of _____ (hereafter referred to as “the Carrier”) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Carrier and Customs is intended to enhance the joint efforts of both entities in developing a more secure border environment by improving the security for the transportation of passengers, crew, conveyances and cargo throughout the commercial process. Customs and the Carrier recognize the need to improve and expand existing security practices in order to achieve a more efficient and compliant import process.

The Carrier agrees to develop and implement, within a framework consistent with the listed recommendations, a verifiable, documented program to enhance security procedures throughout its supply chain process. Where the Carrier does not exercise control of a production facility, distribution entity, or process in the supply chain, the Carrier agrees to communicate the attached recommendations/guidelines to those entities.

Specifically, the Carrier agrees to:

1. Complete and return the attached Sea Carrier Supply-chain, security profile questionnaire within 60 days of signing and returning the agreement to Customs. Upon request from the carrier, an extension, not to exceed 30 days, may be granted to complete the security questionnaire.
2. Prior to arrival at first U.S. port, search the vessel, prepare a vessel search checklist, and secure all areas as appropriate.
3. Designate a liaison representative in each port where the carrier operates for Customs to contact.
4. Designate a vessel officer as liaison for Customs to contact.
5. Establish a security system for cargo storage and handling facilities, container yards and vessels operated by the carrier. Customs physical and procedural security recommendations should be used as a reference.
6. Establish system of security for each vessel to include:
7. Control all access to vessel while in port.
8. All persons boarding the vessel must be identified as having a legitimate reason to be onboard.
9. Deny access to all non-essential personnel.
10. While at port, the pier and waterside of vessel must be adequately illuminated.
11. Limit shore employees and service providers to those areas of the vessel where they have legitimate business.
12. Ensure that contract companies who provide vessel related services (e.g., contract security) commit to C-TPAT Security Recommendations. Periodically review the

security commitments of the service providers to detect weakness, or potential weaknesses, in security.

13. Credentialing and background checks of employees will be conducted as required by applicable federal and state statutes and regulations.
14. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to Customs upon written request, to the extent permitted by law.
15. Ensure that all manifest/bills of lading and other documentation submitted for cargo to be shipped are complete.
16. Establish programs or procedures to safeguard its information systems, documents and forms from unauthorized use.
17. Provide Customs with requested data/information about cargo or container movements, provided that the number and nature of such requests from Customs shall not be unreasonably burdensome. Customs recognizes the highly confidential and proprietary nature of such information, and agrees to take appropriate steps to maintain the confidentiality of this information.
18. Ensure high security seals or locks are affixed on all loaded containers.
19. Visually inspect all empty containers, to include the interior of the container, at the foreign port of lading.
20. Participate with Customs in joint security surveys at selected facilities both abroad and in the United States.
21. Provide Customs, upon request, with documentation that demonstrates compliance with each item of this agreement.
22. Participate in the Automated Manifest System. Provide Customs with advance arrival copies of cargo manifest and bills of lading.
23. Notify Customs of shippers/cargoes with irregular profiles as defined by Customs.
24. Require, as a matter of Carrier policy, that all of its employees cooperate fully with Customs in implementing the various actions and initiatives of C-TPAT.
25. Conduct periodic unannounced security checks to ensure that all procedures are being performed.
26. A security awareness program should be developed and 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.
27. To the extent possible and where feasible, cooperate with U.S. Customs, domestic and foreign port authorities, foreign customs administrations, and other industry leaders, in advancing the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI).

Specifically, Customs agrees to:

1. Acknowledge that the prime responsibility of the Carrier lies in the safe and expeditious movement of cargo and the facilitation, to the greatest extent possible, of the Carrier's legitimate business concerns, not that of a law enforcement agency.
2. Consider the Carrier's acceptance and implementation of the listed guidelines when making risk determinations for the purposes of cargo examinations and document reviews.
3. Review the Carrier's application package and provide feedback and recommendations to the Carrier on the information provided in the Security Profile Questionnaire within 60 days of receipt.
4. Conduct initial and periodic conveyance, facility and procedural surveys. All surveys will include a report from Customs on its findings and suggestions for improvements.
5. A joint security awareness program should be developed in conjunction with the carrier and 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.
6. Will not request that the Carrier take any action, which will conflict with the laws, regulations, or control requirements of any country.
7. Assist the Carrier in identifying high-risk ports, routes, and facilities, and in assessing its vulnerability to terrorism.
8. Participate with the Carrier in joint security surveys at the selected facilities both abroad and in the United States.
9. Assign the carrier a Customs account manager and provide a point of contact at each United States port served by the Carrier for all matters relative to this Agreement.
10. Coordinate, with Carrier management, press releases or information to the public, which directly involve the Carrier's interest. The joint and cooperative nature of this Agreement will be emphasized.
11. Distribute to carrier C-TPAT participants cleared information regarding security threats, exposures and trends.

The listed Security Recommendations reflect the mutual understanding of the Carrier and Customs of what constitutes the appropriate elements of the carriers supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Carrier.

This Agreement is subject to review by the Carrier or Customs and may be altered by mutual agreement or terminated with written notice by either party.

This Agreement cannot, by law, exempt the Carrier from any statutory or regulatory sanctions in the event that discrepancies are discovered during a physical examination of cargo or the review of documents associated with the Carrier Customs transactions.

Nothing in this Agreement relieves the Carrier of any responsibilities with respect to United States law, including the Customs Regulations.

Name & Title
United States Customs

Name & Title
Service Company



Required Documentation: Sea Carrier - C-TPAT Supply Chain Security Profile Questionnaire

1.) Provide an executive summary outlining the process elements of the security procedures you currently have in place. At minimum, address the following elements:

- Security Program:
 1. Facilities security.
 2. Theft prevention.
 3. Shipping and receiving controls.
 4. Information security controls - integrity of automated systems.
 5. Internal controls - process established for reporting and correcting problems.

- Personnel Security:
 1. Pre-employment screening & periodic background reviews.
 2. Employee training on security awareness and procedures.
 3. Internal codes of conduct.
 4. Internal controls - process established for reporting and managing problems related to personnel security.

- Service Provider Requirements:
 1. Written standards for service providers' physical and procedural security.
 2. Internal controls for the selection of service providers.
 3. Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti-Smuggling Coalition (BASC).

2.) Indicate that the specific detailed procedures noted above are available to Customs in a verifiable format at an identified location.

- Include an assessment of your security processes, as well as information on what changes you envision making to improve security.

Identifying perceived weaknesses or gaps will not necessarily prohibit participation in C-TPAT. Customs is committed to working with you to identify effective corrections and adjustments to your processes that will result in a more secure supply chain operation. We have specific programs in place that can assist your company in meeting this objective. Our Industry Partnership Program (IPP) Coordinators can provide expert advice on establishing security programs throughout your supply chain. Program information will be provided upon request.



Rail Carrier

Rail Carrier Security Recommendations for C-TPAT

Rail 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 un-manifested 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 un-manifested 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.



Rail Carrier Instructions for C-TPAT

To apply for participation in the C-TPAT, follow the instructions noted below to complete the Rail Carrier Agreement to Voluntarily Participate and the Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT “Fact Sheet” is available to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions please contact U.S. Customs Industry Partnership Programs at industry.partnership@customs.treas.gov

Instructions:

Review and sign the “Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism.” This represents the applicant’s commitment to the C-TPAT security recommendations and the applicant’s commitment to work with its service providers throughout its supply chain to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.

Return two original signed Agreements to:

**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**

Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:

- Official Company Name
- Street Address, including zip code
- Company Point of Contact to include:
 - Name of Point of Contact and title
 - Telephone Number
 - Fax Number
 - E-mail Address
 -

Complete the Supply-chain, security profile questionnaire and additionally:

Mail an electronic copy contained on a 3.5” floppy disk or a CD-ROM to the address listed in item number 2.

Or

E-mail a copy to industry.partnership@customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire”

The following guidance is provided to better inform you on how to complete the Supply Chain Security Profile Questionnaire:

The focus of the profile should be on the Carrier’s Supply Chain, including the foreign countries you operate in and/or conduct business.

The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes and confirm that they have an active security program in place.

NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to Customs as part of the profile response.

Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti-Smuggling Coalition (BASC).

Upon receipt, Customs will review the carrier’s completed Supply Chain Security Profile Questionnaire. After Customs completes its review, the carrier will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on its application within 60 days.

An electronic confirmation indicating receipt of a signed agreement will be sent to the e-mail address provided in the application.



Required Documentation: Rail Carrier - C-TPAT Agreement to Voluntarily Participate

This Agreement is made between _____, of _____ (hereafter referred to as “the Carrier”) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Carrier and Customs is intended to enhance the joint efforts of both entities in developing a more secure border environment by improving the security for the transportation of passengers, crew, conveyances and cargo throughout the commercial process. Customs and the Carrier recognize the need to improve and expand existing security practices in order to achieve a more efficient and compliant import process.

The Carrier agrees to develop and implement, within a framework consistent with the listed recommendations, a verifiable, documented program to enhance security procedures throughout its supply chain process. Where the Carrier does not exercise control of a production facility, distribution entity, or process in the supply chain, the Carrier agrees to communicate the attached recommendations/guidelines to those entities.

Specifically, the Carrier agrees to:

1. Complete and return the attached Rail Carrier Supply-chain, security profile questionnaire within 60 days of signing and returning the agreement to Customs. Upon request from the carrier, an extension, not to exceed 30 days, may be granted to complete the security questionnaire.
2. Prior to arrival at first U.S. port, conduct a comprehensive security search of all equipment under Carrier control.
3. Maintain and/or establish security systems for foreign and domestic cargo storage and handling facilities, container yards and conveyances operated by the Carrier.
4. Where the Carrier operates facilities in a foreign country, establish security procedures designed to restrict access to conveyances and equipment.
5. The Carrier is encouraged to develop and utilize a photo identification system for employees and require visitors to display proper identification. Employees and visitors should only be permitted access to cargo, facilities and conveyances under Carrier control when required by their duties.
6. Credentialing and background checks of employees, normally assigned to work at the Carrier’s facilities along the Mexican and Canadian borders, will be conducted as required by appropriate federal and state statutes and regulations.
7. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to Customs upon written request, to the extent permitted by law.

8. Require, as a matter of Carrier policy, that all of its managers, supervisors, employees and representatives cooperate with Customs and other applicable law enforcement entities.
9. Implement systems designed to ensure that all manifest/bills of lading and other documentation (including electronic data transmissions) submitted for cargo to be shipped are complete and implement systems designed to ensure the integrity of Carrier seals.
10. Report to Customs suspicious shippers, shipping practices, or when anomalies appear in shipping documentation or railroad equipment.
11. Designate a Carrier official or representative to serve as a liaison with Customs at each port of entry served by the Carrier.
12. A security awareness program should be developed and 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.
13. Provide Customs with access to the Carrier's systems for the purpose of identifying and tracking railroad equipment and shipments that, according to profiles developed by Customs, have a relatively high probability of being used to transport contraband by rail into the United States. Customs shall not be unreasonably burdensome. Customs recognizes the highly confidential and proprietary nature of such information, and agrees to take appropriate steps to maintain the confidentiality of this information.
14. To the extent possible and where feasible, cooperate with U.S. Customs, domestic and foreign port authorities, foreign customs administrations, and other industry leaders, in advancing the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI).

Specifically, Customs agrees to:

1. Review security procedures developed by the Carrier and, if necessary, offer recommendations for improvement.
2. Provide informational support to the Carrier's Police Department, or designated security representative, on security and drug smuggling issues, including, where practicable, information on the use of (a) certain types of equipment and/or (b) particular corridors or crossing points, for the conveyance of un-manifested cargo, illegal drugs or contraband.
3. Coordinate with the Carrier's management the release of information to the media or general public on matters relating to this Agreement.
4. Provide assistance, when feasible, to the Carrier with inspections of its conveyances through the use of special equipment and personnel.
5. Consider the Carrier's acceptance and implementation of the listed guidelines when making risk determinations for the purposes of cargo examinations and document reviews.

6. Will not request that the Carrier takes any action, which will conflict with the laws, regulations, or control requirements of any country.

The listed Security Recommendations reflect the mutual understanding of the Carrier and Customs of what constitutes the basic elements of the carrier's supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Carrier.

This Agreement is subject to review by the Carrier or Customs and may be altered by mutual agreement or terminated with written notice by either party.

This Agreement cannot, by law, exempt the Carrier from any statutory or regulatory sanctions in the event that discrepancies are discovered during a physical examination of cargo or the review of documents associated with the Carrier Customs transactions.

Nothing in this Agreement relieves the Carrier of any responsibilities with respect to United States law, including the Customs Regulations.

Name & Title
United States Customs

Name & Title
Service Company



Required Documentation: Rail Carrier - C-TPAT Supply Chain Security Profile Questionnaire

1.) Provide an executive summary outlining the process elements of the security procedures you currently have in place. At minimum, address the following elements:

- Security Program:
 1. Facilities security.
 2. Theft prevention.
 3. Shipping and receiving controls.
 4. Information security controls - integrity of automated systems.
 5. Internal controls - process established for reporting and correcting problems.
- Personnel Security:
 1. Pre-employment screening & periodic background reviews.
 2. Employee training on security awareness and procedures.
 3. Internal codes of conduct.
 4. Internal controls - process established for reporting and managing problems related to personnel security.
- Service Provider Requirements:
 1. Written standards for service providers' physical and procedural security.
 2. Internal controls for the selection of service providers.
 3. Indicate if your service providers participate in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), the Business Anti-Smuggling Coalition (BASC).

2.) Indicate that the specific detailed procedures noted above are available to Customs in a verifiable format at an identified location.

- Include an assessment of your security processes, as well as information on what changes you envision making to improve security.

Identifying perceived weaknesses or gaps will not necessarily prohibit participation in C-TPAT. Customs is committed to working with you to identify effective corrections and adjustments to your processes that will result in a more secure supply chain operation. We have specific programs in place that can assist your company in meeting this objective. Our Industry Partnership Program (IPP) Coordinators can provide expert advice on establishing security programs throughout your supply chain. Program information will be provided upon request.



C-TPAT Frequently Asked Questions - Air, Rail, and Sea Carriers

Q: Is C-TPAT a voluntary program for carriers?

A: Yes. C-TPAT will build upon existing relationships with the transportation industry, to enlist voluntary carrier participation in the program and enhance the security “best practices” employed by carriers.

Q: What carriers are eligible to participate in C-TPAT?

A: All common commercial air, rail, and sea carriers are eligible to enroll in C-TPAT beginning July 15, 2002, including, air passenger and cargo carriers, express consignment carriers, and ocean container and bulk carriers.

Q: How will C-TPAT become available to the trucking industry?

A: Along our northern border, the U.S. Customs Service is working with our Canadian counterparts to create a harmonized processing system to be used in conjunction with U.S. and Canadian industry partnership programs. This program, currently being referred to as “FAST” (Free and Secure Trade) will provide the platform for implementation of C-TPAT along the northern border and will include the conduit for trucking companies to enroll into the program. We expect this process to be in place within the very near future.

The U.S. Customs Service is working with our Mexican counterparts to create a more secure and efficient processing system along the southwest border, much like our efforts with Canada. C-TPAT for trucking companies along the U.S.-Mexico border will build upon the industry partnership programs already established in the region.

Q: As a carrier, I already participate in the Customs Carrier Initiative Program. Is it a duplication of effort in joining C-TPAT?

A: C-TPAT participation will not require duplicate work for current Customs Carrier Initiative Program (CIP) participants. Customs will be looking for carriers to join C-TPAT and enhance existing security practices to better address the terrorism threat to international air, sea, and land shipping. CIP participants already subscribe to the importance of security from a narcotics-smuggling perspective and are well positioned to expand their security focus to encompass an anti-terrorism approach.

Q: Will the Air and Sea Carrier C-TPAT agreements apply to all distinctions of carriers within the specific transportation group?

A: Yes. Like the CIP agreements, one comprehensive C-TPAT agreement will apply to all distinctions of carriers within one transportation sector. Accordingly, an airline or sea carrier will only be responsible for those elements of the C-TPAT agreement that apply to their individual operation. For example, if your airline does not carry cargo, you will not be expected to implement the elements of the agreement that address cargo security. In the maritime environment, if you are purely a bulk cargo operation, those elements of the C-TPAT sea carrier agreement pertaining to containers will not apply.

Q: Are there monetary penalties associated with C-TPAT?

A: No.

Q: Will C-TPAT replace the Carrier Initiative Programs?

A: C-TPAT will serve as the umbrella program for all USCS Industry Partnership Programs. For the near term, the Carrier Initiative Programs and C-TPAT will co-exist as two similar but separate Customs Industry Partnership programs. The most notable distinction being that the issuance of drug penalties under existing regulations, and the mitigation provisions for current carrier initiative participants, will continue to be administered under the CIP agreements.

Q: As an active member of the Carrier Initiative Program, am I automatically enrolled into C-TPAT?

A: No. Because C-TPAT entails higher security practices and a broader scope (e.g., terrorism), in order to realize C-TPAT benefits, each carrier must enroll into C-TPAT by signing the appropriate agreement, and submit a completed Carrier Supply Chain Security Profile Questionnaire.

However, because active CIP participants already subscribe to stringent security standards throughout the scope of their operations, it is anticipated that these carriers will rapidly meet the standards of C-TPAT thus expediting the enrollment process and realization of benefits. For current Super Carrier Initiative participants, the process will be yet more streamlined.

Q: What additional benefits are there for carriers to join C-TPAT?

A: The more Customs knows about your security, the more effective we will be at making risk determinations concerning your conveyance or operation. Through C-TPAT, Customs will make available to the carrier community benefits not attainable under the Carrier Initiative Programs, including, reduced exams, the assigning of an Account Manager, and expedited processing.

Q: Can I remain in the Carrier Initiative Program and choose not to participate in C-TPAT?

A: Yes. However, for you as a carrier to receive the benefits listed above, you must be C-TPAT certified. In addition, as C-TPAT evolves, USCS plans to eventually phase CIP into C-TPAT beginning with the drug penalty, mitigation process.

For more information:

Contact the Industry Partnership Programs, at (202) 927-0520 or email, at industry.partnership@customs.treas.gov



U.S. Marine Ports and Terminals

U.S. Marine Port/Terminal Security Recommendations for Customs Trade Partnership Against Terrorism (C-TPAT)

Operators should develop and implement a comprehensive plan to enhance port/terminal security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the size and structure of the port/terminal and may not be applicable to all.

Ports/Terminals are encouraged to participate in the U.S. Coast Guard Navigation and Vessel Inspection Circular (NVIC) for waterfront facilities. U.S. Customs and the Coast Guard have worked closely to ensure consistency between C-TPAT

(U.S. Marine Port/Terminal) and the NVIC (waterfront facilities) programs. Customs recognizes the additional guidance that the NVIC program provides regarding port/terminal security and that the tenants of NVIC are consistent with the tenants of C-TPAT.

Access Controls: Unauthorized access to the port/terminal, secure areas within the port/terminal, and vessels moored thereto, should be prohibited. At minimum, controls should include the positive identification of all employees, visitors, and vendors at all access points. Procedures for safely challenging and removing unauthorized/unidentified persons should be in place.

Parking Controls: Parking within the port/terminal secure areas should be controlled and restricted. Parking should be authorized by an adequate gate/pass and/or decal system. Parking for employees, dockworkers and visitors should be restricted to designated areas.

Procedural Security: Port/Terminal operators should have written and verifiable security procedures in place with regards to areas under port/terminal control. Procedures should be in place for notifying Customs and other appropriate law enforcement agencies in cases where anomalies or illegal activities are detected or suspected.

Personnel Security: Employee screening, application verifications, the interviewing of prospective employees and periodic background checks should be conducted, as required by applicable federal and state statutes and regulations.

Security Awareness: A security awareness program should be provided to employees and include instruction on maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

Physical Security: Port/Terminal controlled facilities should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Where appropriate, physical security should include adequate perimeter fencing, interior fencing, gates and gatehouses, signage, CCTV, lighting inside and outside the facility, locking devices on external and internal doors, windows, gates and fences.

Maintenance: A maintenance program comprised of regularly scheduled inspections to keep fencing, gates, lights and cameras in good condition and working order, should be implemented.

Information Security: Measures should be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access. Where applicable, measures should be taken to secure sensitive information in order to prevent the loss or unauthorized use of such information.

Cargo Security: Procedures should be established to control and monitor cargo transfer operations within the port / terminal.



U.S. Marine Port/Terminal Application Instructions for Customs-Trade Partnership Against Terrorism

To apply for participation in the C-TPAT, follow the instructions noted below to complete the Memorandum of Understanding (MOU) and the Supply Chain Security Profile Questionnaire.

For your reference, a C-TPAT “Fact Sheet” is available on our website to answer general questions about the C-TPAT program and potential benefits for participants.

If you have questions, please contact U.S. Customs Industry Partnership Programs at industry.partnership@customs.treas.gov

INSTRUCTIONS:

1. Review and sign the “Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism.” This represents the applicant’s commitment to the C-TPAT security recommendations and the applicant’s commitment to work with its service providers throughout its supply chain to enhance security processes and procedures. The Agreement should be signed by a corporate officer with the authority to implement security enhancements that may be necessitated upon committing to participate in the program.
2. Return two original signed Agreements to:
**United States Customs Service
Office of Field Operations
Industry Partnership Programs
1300 Pennsylvania Avenue, N.W.
Room 5.4C
Washington D.C. 20229
Attention: C-TPAT**
3. Upon submission of your signed agreement, please be sure to also include (on a separate cover) the following:
 - a. Official Company Name
 - b. Street Address, including zip code
 - c. Company Point of Contact to include:
 1. Name of Point of Contact and title
 2. Telephone Number
 3. Fax Number
 4. E-mail Address
4. Complete the Supply-chain, security profile questionnaire and:
 - a. Mail an electronic copy contained on a 3.5” floppy disk or a CD-ROM to the address listed in item number 2.

Or

- b. E-mail a copy to Industry.partnership@Customs.treas.gov and include in the subject line the name of your company and “Security Questionnaire”
5. The following guidance is provided to better inform you on how to complete the Supply Chain Security Profile Questionnaire:
 - a. The focus of the profile should be on the company’s supply chain processes.
 - b. The Security Profile should contain an executive summary outlining the process elements of the security procedures you currently have in place. The Security Profile should also identify the service providers your company utilizes and confirm that they have an active security program in place. (NOTE: Detailed profiles of the security processes utilized by your service providers should not be forwarded to Customs as part of the profile response.)
 - c. Describe your process for communicating C-TPAT security recommendations to your service providers and for promoting service provider participation in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), and/or the Business Anti-Smuggling Coalition (BASC).
6. Upon receipt, Customs will review the company’s completed Supply Chain Security Profile Questionnaire. After Customs completes its review, the company will receive a copy of the Customs-Trade Partnership Against Terrorism Agreement, signed by the Assistant Commissioner, Office of Field Operations, along with feedback on its application within 60 days.



U.S. Marine Port Authority/Terminal Operator Agreement to Voluntarily Participate in Customs-Trade Partnership Against Terrorism

This Agreement is made between _____, of _____ (hereafter referred to as the Port/Terminal) and the United States Customs Service (hereafter referred to as “Customs”).

This Agreement between the Port/Terminal and Customs is intended to enhance the joint efforts of both entities in developing a more secure border environment by improving the security for conveyances, facilities, ports, terminals and cargo throughout the commercial process. Customs and the Port/Terminal recognize the need to improve and expand existing security practices in order to achieve a more efficient and compliant process.

The Port/Terminal agrees to develop and implement, within a framework consistent with the listed security recommendations/guidelines, a verifiable, documented program to enhance security procedures throughout the supply chain process. Where the Port/Terminal does not exercise control of a distribution entity, or process in the supply chain, the Port/Terminal agrees to communicate the attached security recommendations/guidelines to those entities.

Specifically, the Port/Terminal agrees to:

1. Complete and return the attached “U.S. Marine Port/Terminal Security Profile Questionnaire” within 60 days of signing and submitting the C-TPAT U.S. Marine Port/Terminal Agreement to Customs. Upon request from the Port/Terminal, an extension, not to exceed 30 days, may be granted to complete the security questionnaire.
2. Designate a liaison representative in each Port/Terminal for Customs to contact.
3. Establish a security system for Port/Terminal property and related facilities. Customs physical and procedural security recommendations should be used as a reference.
4. Communicate C-TPAT security recommendations to contract companies who provide Port/Terminal related services. Periodically review the security commitments of the service providers to detect weakness, or potential weaknesses, in security.
5. Credentialing and background checks of employees will be conducted as required by applicable federal and state statutes and regulations.
6. Maintain a current permanent employee list to include the name, date of birth, social security number, and position held, for each corporate employee, and submit such information to Customs upon written request, to the extent permitted by law.
7. Establish programs or procedures to safeguard Port/Terminal information systems, documents and forms from unauthorized use.

8. Provide Customs with requested data/information about vessel or container movements, provided that the number and nature of such requests from Customs shall not be unreasonably burdensome.
9. Participate with Customs in joint site surveys at selected facilities both abroad and in the United States.
10. Provide Customs, upon request, with documentation that demonstrates compliance with each item of this agreement.
11. Require, as a matter of Port/Terminal policy, that all of its employees cooperate fully with Customs in implementing the actions and initiatives of C-TPAT including the expanded use of technology.
12. Conduct periodic unannounced security checks to ensure that all procedures are being performed.
13. A security awareness program should be developed and provided to employees. The program should include instruction on maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.
14. To the extent possible and where feasible, cooperate with U.S. Customs, domestic and foreign port authorities, foreign customs administrations, and other industry leaders, in advancing the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI).
15. Ports / Terminals should notify Customs and other appropriate law enforcement agencies whenever anomalies or illegal activities related to security issues are detected or suspected.

Specifically, Customs agrees to:

Customs acknowledges that during the processing of this Agreement, Customs may become privy to confidential information. Customs recognizes the highly confidential and proprietary nature of such information, and agrees to take the appropriate measures to maintain the confidentiality of this information.

1. Acknowledge that the prime responsibility of the Port/Terminal lies in the safe and expeditious movement of cargo and the facilitation, to the greatest extent possible, of the Port's/Terminal's legitimate business concerns, not that of a law enforcement agency.
2. Review the Port's/Terminal's application package and provide feedback and recommendations to the Port/Terminal on the information provided in the Security Profile Questionnaire within 60 days of receipt.
3. A joint security awareness program should be developed in conjunction with the Port/Terminal and provide instruction to employees on recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.
4. Will not request that the Port/Terminal take any action, which will conflict with the laws, regulations, or control requirements of any country.
5. Assist the Port/Terminal in identifying high-risk ports, routes, and facilities, and in assessing its vulnerability to terrorism.

6. Participate with the Port/Terminal in joint site surveys at selected facilities both abroad and in the United States.
7. Assign the Port/Terminal a Customs C-TPAT point-of-contact and at each participating United States Port/Terminal for all matters relative to this Agreement.
8. Coordinate, with Port/Terminal management, press releases or information to the public, which directly involve the Port's / Terminal's interest. The joint and cooperative nature of this Agreement will be emphasized.
9. Distribute to Port/Terminal C-TPAT participants cleared information regarding security threats, exposures and trends.

The listed recommendations/guidelines reflect the mutual understanding of the Port/Terminal and Customs of what constitute the appropriate elements of the Port's / Terminal's supply chain security.

This Agreement will be administered pursuant to a plan jointly developed by Customs and the Port/Terminal.

This Agreement is subject to review by the Port/Terminal or Customs and may be terminated with written notice by either party.

This Agreement cannot, by law, exempt the Port/Terminal from any statutory or regulatory requirements.

Nothing in this Agreement relieves the Port/Terminal of any responsibilities with respect to United States law, including Customs Regulations.

 Name & Title
 United States Customs Service

 Name & Title
 Company

Attachments



U.S. Marine Port Authority/Terminal Operator Security Profile Questionnaire

1.) Provide an executive summary outlining the process elements of the security procedures you currently have in place. At minimum, address the following elements:

- Security Program:
 - Facilities security.
 - Theft prevention.
 - Shipping and receiving controls.
 - Information security controls – integrity of automated systems.
 - Internal controls – process established for reporting and correcting problems.
- Personnel Security:
 1. Pre-employment screening & periodic background reviews.
 2. Employee training programs on security awareness and standard operating procedures.
 3. Internal codes of conduct.
 4. Internal controls – process established for reporting security violations and for managing issues related to personnel security.

2.) Service Provider Requirements

1. Written standards for service providers' physical and procedural security as they relate to Port/Terminal operations.
 2. Internal controls for the selection of service providers.
 3. Describe your process for communicating C-TPAT security recommendations to your service providers and for promoting service provider participation in Customs Industry Partnership Programs: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Carrier Initiative Program (CIP), the Super Carrier Initiative Program (SCIP), and/or the Business Anti-Smuggling Coalition (BASC).
- 3.) Indicate that the specific detailed procedures noted above are available to Customs in a verifiable format at an identified location upon request.
- Include an assessment of your security processes as well as information on what changes you envision making to improve security.
 - Identifying perceived weaknesses or gaps will not necessarily prohibit participation in C-TPAT. Customs is committed to working with you to identify effective corrections and adjustments to your processes that will result in a more secure supply chain operation. We have specific programs in place that can assist your company in meeting this objective. Our Industry Partnership Program (IPP) coordinators can provide expert advice on establishing security programs throughout your supply chain. Program information will be provided upon request.



Warehouse Security Recommendations

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 un-manifested 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.



Manufacturer Security Recommendations

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.