CTPAT Job Aid
Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

CTPAT Virtual Validation Meeting

***** Please be advised that this is a sample agenda and intended for use as a guide to approach and prepare for a CTPAT validation. Since the agenda is not representative of all entities and their Minimum-Security Criteria (MSC), it is incumbent upon the CTPAT partner to review all applicable MSC for their respective entity to ensure compliance.

The Virtual Validation – The Virtual Validation process utilizes video conferencing to securely connect Customs Trade Partnership Against Terrorism (CTPAT) partners and its representatives with the assigned Supply Chain Security Specialist (SCSS) and allows for the safe exchange, review, and validation of pertinent supply chain security data, in a real-time environment. To the extent possible, the virtual validation will mirror the physical validation process, and will include a review of the written documentation, procedures, and security measures implemented to secure the CTPAT partner's international supply chain. Depending on technical capabilities, a review of critical Minimum-Security Criteria (MSC) requirements, to include the physical security of the facility, may be conducted, utilizing the video conferencing platform.

*The Validation process includes the verification of the CTPAT partner's compliance with CTPAT's MSC. The validation process is fundamentally based upon – and requires – **written company policies** governing supply chain security and **evidence of implementation** for the company's security policies.

Written, standard operating procedures (SOP) must be customized to fit the company's international business model. SOPs should be written in a step-by-step, procedural format, to include descriptive detail, and clearly demonstrate the company's active and operational cargo security procedures.

The CTPAT validation meeting serves as the company's opportunity to demonstrate compliant security processes and practices relative to the company's function and/or responsibility within a CTPAT partner's supply chain for shipments destined to the U.S. (e.g., manufacturing cargo, freight forwarding, storage and distribution, brokerage, or importation).

Validation meetings typically last between four and six hours, dependent upon company preparedness and other factors. The appropriate company representatives should be available/on-call to answer questions relative to their area of expertise and responsibility, although they are not required to attend the meeting.

The following CTPAT MSC sections (below) will be addressed during the Validation meeting as they relate to the company's function and/or responsibility within the CTPAT partner's supply chain, with a focus on shipments destined to the U.S.

Primary areas of focus are: (1) Documentation (SOP) that support and demonstrate the company's compliance with CTPAT MSC; (2) *Detailed in the CTPAT MSC weblink (below)*; and (3) Described further in *each* MSC section below.

CTPAT MSC information is detailed at this link (in English and other languages) –
CTPAT Minimum Security Criteria and Guidelines

CTPAT Job Aid
Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

Following introductions by representatives from the company and CTPAT, the validation meeting will begin with a discussion focused on the company's business model, and then will lead to a discussion and review of the security measures that the company has implemented into its daily operations.

Following the review of the company's security measures, the SCSS may 'virtually' tour the facility to visually observe physical security procedures. The meeting will end with a brief close-out discussion and a review of the findings by the CTPAT validation team. If compliant security processes and practices are not in place in any key areas, the team will discuss possible solutions to meet CTPAT MSC as detailed in the link above and as described further below.

– The MSC sections below describe CTPAT compliance measurements that are reviewed –

* The Validation meeting will be most productive if the company, to the extent possible, has *all documents and SOPs (listed below, as applicable)* available for review during the meeting *

** You may utilize this Meeting Agenda as a guideline – to (electronically) insert/embed the corresponding SOP or document (.doc or .pdf) icon into each appropriate bulleted section. Simply click the area where you want to insert your SOP, click "Insert" at the top left side of the header, then click "Object" at the top right side of the header. The Object box will pop up. Click "Create from File", check the "Display as Icon" box, then click "Browse". Double-click the SOP or document you want to insert and click OK.*

- **Corporate Security – Security Vision and Responsibility**

Please be prepared to discuss upper management's support of the CTPAT supply chain security program, as well as the company's internal audit process.

– Company management (or designated CTPAT Team) must have active oversight of the company's security program and the CTPAT Portal account.
– Company management (or designated CTPAT Team) must be knowledgeable with CTPAT requirements.
– The company's CTPAT security program must be supported by a written review component (i.e., SOP for audits/updates of the company's written policies and security procedures).
– The company's CTPAT security program should be supported by a *Statement of Support*.

* Documentation that details and demonstrates the company's security vision and responsibility procedures and the company's internal audit process should be available for review by the CTPAT validation team during the meeting *

- **Corporate Security – Risk Assessment**

Please be prepared to discuss the company's risk assessment (RA) process.

– The company must conduct an overall risk assessment to identify security vulnerabilities.
– The company must conduct and document the amount of risk in its international supply chain(s).
– The company's risk assessment must be supported by a written SOP (detailing the RA process).
– The company should follow the CTPAT 5-Step Risk Assessment process.
– The risk assessment should include a documented cargo/shipment mapping process.

* Documentation that details/demonstrates the company's risk assessment process should be available for review, by the CTPAT validation team during the meeting *

- **Corporate Security – Business Partners**

Please be prepared to discuss the company's Business Partner screening process.

– The company must have a written SOP that documents the risk-based process to screen new business partners and to monitor its current business partners.

* Based upon the company's international business model and the company's function and/or the company's responsibility within the CTPAT partner's supply chain*

– The Screening process must include the company's key business partners.

* Key business partners are designated based upon the criticality of their function and/or responsibility within the supply chain. Key business partners include those involved with the manufacture, security and/or the facilitation of cargo/shipments destined to the U.S. (e.g., vendors and suppliers (not raw material suppliers), logistics and transportation service providers, freight forwarders, security guards, customs brokers).

– The company's written screening SOP that documents the process must be structured to identify specific risk factors (i.e., warning indicators/red flags, non-compliant security procedures, CTPAT or AEO certification).

* Documentation that details/demonstrates the company's Business Partner Screening and Auditing process should be available for review by the CTPAT validation team during the meeting *

CTPAT Job Aid
Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

- **Corporate Security – Cybersecurity**

Please be prepared to discuss the company's cybersecurity procedures and policies.

– The company must have a written SOP for cybersecurity procedures and policies in place to protect the company's IT information technology systems.
– The company's cybersecurity/IT SOP must be reviewed and updated at least annually.
– The company's cybersecurity/IT SOP must include procedures to prevent attacks via social engineering.
– The company must train relevant employees regarding cybersecurity/IT policies and procedures.
– The company's employee(s) who manage cybersecurity/IT security technology systems must receive training.
– The company must document employee training received (e.g., roster sheet, training log, database).
– The company's employees must use individual user accounts and unique passwords.
– The company must have password rules and employees must use strong passwords.
– The company's cybersecurity/IT computer user access must be restricted and based on employee job description or their assigned duties.
– Authorized user access must be reviewed by the company on a regular basis to ensure access to sensitive systems is based on the user's job requirements.
– The company's cybersecurity/IT system and computer workstations must be protected by anti-virus and firewall software. The software must receive regular security updates.
– If a data breach occurs, or an event results in the loss of data and/or equipment, the company's cybersecurity/IT security procedures must include the recovery or replacement of IT systems and/or data.
– The company must have a system in place to identify unauthorized access of company IT systems or data.
– The company must have a system in place to identify the abuse of IT policies and procedures, including improper access of internal systems, or external websites, and tampering or altering of business data by employees, or contractors.
– The company must have written disciplinary actions (SOP) for violators of company IT policies and procedures.
– The company's IT infrastructure security must be regularly tested.
– The company's cybersecurity/IT policies and procedures must apply to employees who are allowed to use personal devices to conduct company work.
– The company's cybersecurity/IT policies and procedures must apply to users who are allowed to remotely connect to the network.
– The company must utilize secure technologies, such as virtual private networks (VPNs) to allow employees to access the company intranet securely, when located outside of the office.
– The company's cybersecurity/IT security procedures must be designed to prevent remote access from unauthorized users.

* Documentation that details/demonstrates the company's cybersecurity procedures should be available for review by the CTPAT validation team during the meeting *

CTPAT Job Aid
Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

- **Transportation Security – Conveyance and Instruments of International Traffic (IIT) Security**

Please be prepared to discuss how the company processes cargo and shipments, including security procedures for the storage of ready-to-ship cargo, loading procedures, inspecting instruments of international traffic (IIT), such as containers *or* trailers, seal protocols, and shipment tracking and monitoring.

* If the company does not physically handle cargo or shipments (e.g., customs brokers)
– and/or –
* If the company outsources or contracts any elements of Conveyance and IIT Security
– and/or –
* If the company is not responsible for performing any elements of Conveyance and IIT Security
– Please be prepared to discuss how the company ensures CTPAT MSC-compliant procedures are in place.

(As applicable) – The CTPAT validation team will review how cargo is secured at point of origin (prior to loading), the loading process, how IIT are inspected prior to loading (e.g., 7-8 or 17-point inspections), how loaded IIT are sealed, how IIT are stored, and how the loaded IIT is tracked and monitored from the factory (or point of loading) to the port/terminal by the company.

(As applicable)
– IIT (e.g., shipping containers, trailers, and box trucks) must be inspected prior to loading.
– The company must have a written SOP for security inspections of IIT.
– The company should document IIT inspections (e.g., inspection checklist).
– Seals utilized to secure IIT must be ISO 17712 compliant.
– Seal inventory must be controlled, and seal protocols must be in place.
It is understood that air shipments to the U.S. may not utilize containers or seals
– The company must have a written SOP for seal protocols.
– Conveyances and IIT must be stored in a secure area to prevent unauthorized access.
– The company should have a written SOP for IIT Storage.
– The company should work with logistics and transportation service providers to track conveyances and shipments from origin to the port/terminal or final destination point.
– The company should have a written SOP for tracking and monitoring.

* Documentation that details/demonstrates the company's Conveyance and IIT Security procedures should be available for review by the CTPAT validation team during the meeting *

- **Procedural Security – Reporting and Notification Protocols**

Please be prepared to discuss the company's procedures to report security incidents and suspicious activities.

– The company must have a written SOP for reporting instructions/protocols (i.e., for a shipment security breach).

– The company's written SOP for reporting instructions/protocols must include a notification contact information list.
– The company's employees must be trained regarding reporting instructions/protocols.
– Following a significant security incident, the company must initiate a post-incident analysis (PIA)
– The company's PIA findings must be documented and made available to the SCSS.
– The company's procedures for reporting instructions/protocols must be disseminated to key business partners.

* Documentation that details/demonstrates the company's Reporting and Notification procedures should be available for review by the CTPAT validation team during the meeting *

- **Procedural Security – Shipment Processing – Documentation**

Please be prepared to discuss the company's role in processing (or facilitating) a typical shipment, including how the shipping process begins, how shipment data is received, how shipment data is verified, how shipping documents are cross-referenced to ensure accuracy, and how the shipping data is submitted to US Customs and Border Protection (CBP).

* Please have a shipping documentation package available for review by the CTPAT validation team, to include all shipping documents maintained that are relative to the processing of a shipment (e.g., purchase order, invoice, packing list, bill of lading (BOL), customs clearance, delivery order, etc.) *

* The document package should include documents from a recent shipment imported into the U.S., as applicable, and it is preferred that the package be specific to the supply chain being reviewed for the current validation *

– The company must have a written SOP for processing (or facilitating) a typical shipment.
– The company must ensure shipping documentation protocols are in place at origin.
– The company and relevant employees must be trained to review shipping documents, identify anomalies and/or suspicious shipments.

* Documentation that details/demonstrates the company's shipment processing procedures should be available for review by the CTPAT validation team during the meeting *

- **Procedural Security – Shipment Processing – Cargo and Shipment Receiving**

(As applicable) – Please be prepared to discuss the company's role in receiving cargo and shipments, including how drivers are positively identified, how container and seal numbers are verified prior to unloading, how cargo is reconciled during the unloading process, and how discrepancies and anomalies are identified, investigated, resolved, and reported (as appropriate).

* If the company does not physically handle cargo or shipments (e.g., customs brokers)
– and/or –
* If the company outsources or contracts any elements of cargo and shipment receiving
– and/or –
* If the company is not responsible for performing any elements of cargo and shipment receiving
– Please be prepared to discuss how the company ensures CTPAT MSC-compliant procedures are in place.

(As applicable) –

– The company must have a written SOP for cargo and shipment receiving.
– The company must have a written SOP to address discrepancies and anomalies.
– The company must have a written SOP for reporting instructions/protocols (i.e., for a shipment security breach).
– The company's procedures for reporting instructions/protocols must be disseminated to its key business partners.

* Documentation that details/demonstrates the company's cargo and shipment receiving procedures should be available for review by the CTPAT validation team during the meeting *

- **Transportation Security – Agricultural Security**

– The company must have a written SOP for agricultural inspections of IIT.

* Documentation that details/demonstrates the company's Agricultural Security procedures should be available for review by the CTPAT validation team during the meeting *

- **People and Physical Security – Physical Security**

Please be prepared to discuss and demonstrate the company's facility security.

– The facility must have physical barriers and/or deterrents that prevent unauthorized access.
– The facility must have adequate lighting inside and outside the facility.
– The company should have a written SOP for facility security.
– The company should have a written SOP for facility inspections.
– The company should document facility inspections (e.g., inspection checklist).

(As applicable) –

* If the facility has a gate(s) where vehicles and/or personnel enter or exit

– The facility gate(s) must be manned and/or monitored.

(As applicable) –

* If the facility is monitored by an intrusion alarm system
– and/or –
* If the facility is monitored by a video surveillance camera system –

– The facility's alarm and/or cameras must be physically secured from unauthorized access.
– The company must have a written SOP governing the authorized use, maintenance (inspections for proper operation), and protection of security technology (alarm and cameras).
– The company's written security technology SOP must be reviewed and updated annually.
– The company's cameras must be positioned to cover key areas of the facility that pertain to the shipping process.
– Designated company personnel (e.g., management, security) must conduct random reviews of camera footage to verify if cargo security procedures are being properly followed in accordance with law.

* Documentation that details/demonstrates the company's facility security procedures should be available for review by the CTPAT validation team during the meeting *

- **People and Physical Security – Physical Access Controls**

Please be prepared to discuss and demonstrate the facility's physical access controls, including:

– How the company controls the movement of employees and visitors throughout the facility.
– How the company positively identifies employees and visitors.
– How the company controls employee access to restricted areas.
– The process utilized to accept visitors, service providers, and drivers.

– The company must have a written SOP for the issuance/activation and retrieval/deactivation of access devices (e.g., identification (ID) badges, radio frequency identification (RFID) cards, hardcopy keys, alarm codes and information technology (IT) access).
– The company must have a written SOP for reporting instructions/protocols (i.e., for unauthorized persons).

(As applicable) – Examples of the following items must be available for review, including:

– Employee ID badge
– Employee RFID card
– Company Property Form and/or Exit Checklist
– Visitor ID badge
– Visitor Log, Driver Log, Warehouse/Shipment Receiving Log
– Work instructions (SOP) for Security Guards

* Documentation that details/demonstrates the company's physical access control procedures should be available for review by the CTPAT validation team during the meeting *

- **People and Physical Security – Personnel Security**

Please be prepared to discuss how the company screens prospective employees and how the company periodically checks current employees.
– The company must have a written SOP for employee screening.
– The company must verify employee data (i.e., application information, employment history, references).
– The company should utilize an employee data verification checklist or similar.
– The company should maintain employee data and screening information in individual files.
– The company should conduct employee background screenings and periodic re-investigations.
– The company must have a written SOP pertaining to employee code of conduct.
– The company must have a written SOP for employee termination.

* Please have a sample employee file available for review *

* Documentation that details/demonstrates the company's personnel security procedures should be available for review by the CTPAT validation team during the meeting *

- **People and Physical Security – Education, Training and Awareness**

Please be prepared to discuss the company's education, training, and security awareness program.

– The company must have an employee security training and threat awareness program in place.
– Company employees must be trained to report security incidents and suspicious activities.
– The company should provide employees with an anonymous reporting method (e.g., suggestion box or hotline).
– The company must train relevant employees to review shipping documents, identify anomalies, and identify suspicious shipments.
– The company should train relevant employees to identify the warning indicators of trade-based money laundering and terrorism financing.
– The security training and threat awareness program must include all CTPAT security requirements.
– The company must have specialized training for sensitive job positions.
– The company must conduct periodic refresher training.
– The company must document employee training received (e.g., roster sheet, training log, database).
– The company should have a written SOP for the education, training, and security awareness program (e.g., trainer, audience, agenda, frequency, training materials).

(As applicable) –

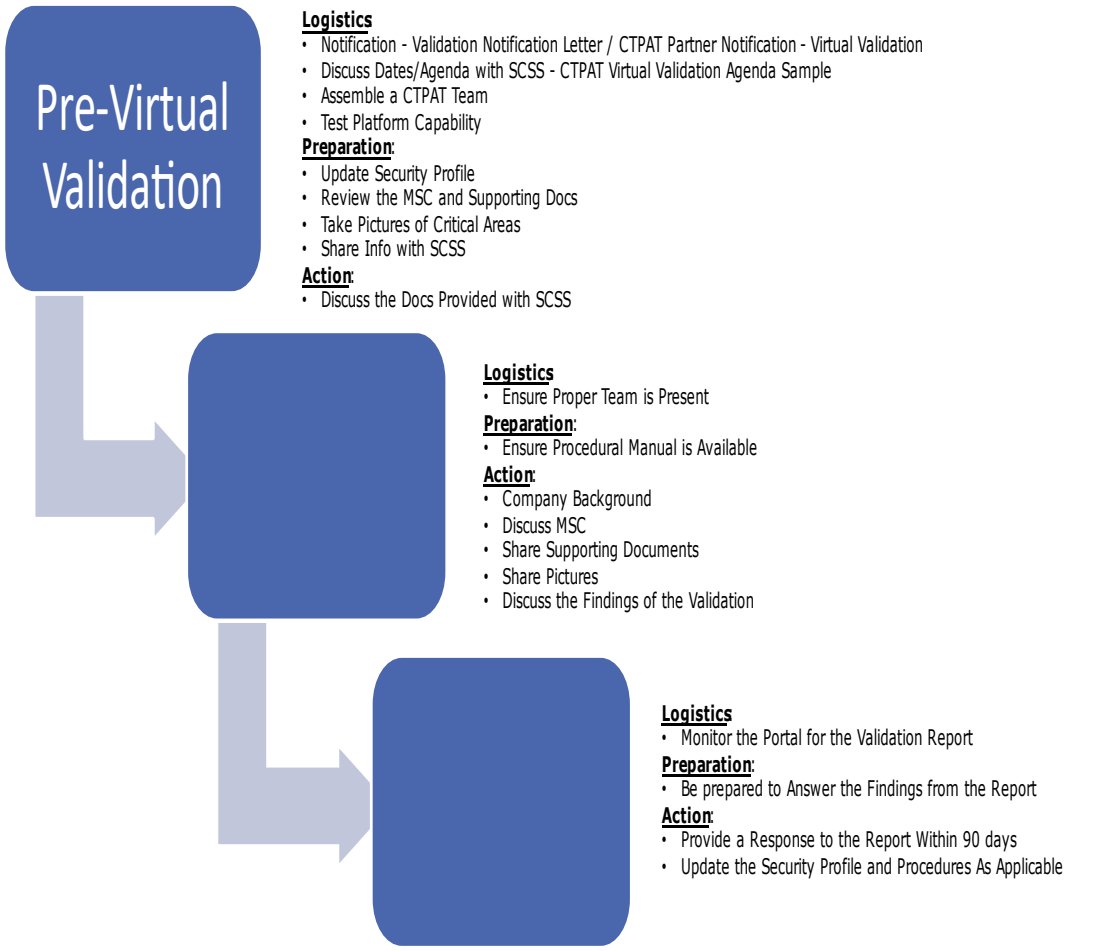
– The company must train relevant employees regarding company cybersecurity/IT policies and procedures.
– The company's employee(s) who manage IT security technology systems must have received training.
– The company must train relevant employees to conduct security and agricultural inspections of empty conveyances and IIT (i.e., containers, trailers).
– The company's conveyance and IIT inspection training must include the following topics: concealment of contraband in hidden compartments (and naturally occurring compartments), signs of pest contamination, and compliance with wood packaging material (WPM).

* Documentation that details/demonstrates the company's education, training and security awareness procedures should be available for review by the CTPAT validation team during the meeting *

CTPAT Job Aid
Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

Virtual Validation Roadmap



1

CTPAT Job Aid

Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

SAMPLE CTPAT VIRTUAL VALIDATION INVITATION LETTER

1300 Pennsylvania Ave. NW, Rm. 2.2A
Washington, DC 20229

U.S. Customs and Border Protection

Date

POC Name
POC Title
Company Name
Address

Dear Mr./Mrs./Ms. POC Name:

As a trusted CTPAT partner with a demonstrated history of compliance with the program's Minimum Security Criteria and CBP laws and regulations, Company Name has been selected to undergo a virtual validation. This innovative approach to the validation process seeks to build on our existing partnership and current benefits, reduce public-private sector costs associated with the on-site visit, and leverage available technology to provide an alternative to traditional methods of supply chain verification that has adaptability across the various business sectors and trade lanes.

What is a Virtual Validation?

The virtual validation will include close collaboration between the CTPAT partner and the Supply Chain Security Specialist (SCSS) in the utilization of available technology to hold virtual meetings, perform domestic and foreign supply chain verifications as applicable, determine compliance with CTPAT's Minimum Security Criteria, and identify and address risk within the supply chain. The virtual validation process will make use of web and video conferencing applications to securely connect the company and its corresponding supply chain facilities with the SCSS and allow for the safe exchange, review, and validation of pertinent supply chain security data in a real-time environment.

What to Expect Next

Your SCSS will be contacting you in the near future to discuss the scope of the virtual validation process, which will include confirmation of the company's ability to perform and utilize this benefit, as well as a request for any supplemental information that may be needed. Once the document review has been completed and the virtual validation date and time agreed upon, the SCSS will invite the company and its selected attendees to commence the virtual validation process.

The Virtual Validation

To the extent possible, the virtual validation will mirror the physical validation process and will include a review of the written documentation, procedures, and security measures implemented to secure the CTPAT partner's international supply chain. Depending on the technical capabilities available, a more immersive review of critical Minimum Security Criteria requirements, to include the physical security of the facility, may be conducted utilizing the web and video conferencing application.

CTPAT Job Aid
Virtual Validation Sample Agenda and Roadmap

Last Updated: October 18, 2021

Virtual Validation Follow-Up and Report

Upon completion of the virtual validation, the CTPAT partner and the SCSS will discuss the findings and evaluate the effectiveness of the partner's security measures, noting any weaknesses or deficiencies that need to be addressed. The virtual validation findings will be documented in the validation report and forwarded to the CTPAT partner for review, and will include any identified supply chain security recommendations or best practices.

We thank you for your continued support and demonstrated compliance with the CTPAT program's Minimum Security Criteria and look forward to partnering with you in this endeavor to adapt to the challenges presented by a dynamic global economy and the escalating threat of terrorism and smuggling.

Sincerely,

Manuel A. Garza, Jr.
Director, CTPAT
Office of Field Operations
U.S. Customs and Border Protection

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229