intertek
Total Quality. Assured.

YOUR PERFECT SOLUTION TO ENHANCED SUPPLY CHAIN SECURITY

STANDARDS & GUIDANCE GLOBAL SECURITY VERIFICATION

Fifth Edition, June 2020

GLOBAL SECURITY VERIFICATION

CONTENTS

I. SCOPE AND BENEFITS

The document provides the following information on the standard:

1. **Intent:** Describes the intent of each element in the GSV 2.0
2. **Program Requirements:** Summarizes the core program requirements
3. **Implementation / Indicators for Achieving Compliance:** Describes key tasks to be implemented to show evidence of compliance

The following section outlines criteria, guidelines, and benefits of a facility's participation in Intertek's Global Security Verification program GSV 2.0.

1. About the standard

After the events of September 11, 2001, governments and customs organizations around the world implemented new supply chain security standards. These secure trade flows, combat illegal trafficking, and protect the security and safety of people and companies doing business around the world. The enhanced supply chain security standards and criteria, including CTPAT, PIP and AEO, have been recognized and implemented by the global trade community. As part of enforcing and adhering to the international supply chain security standards, companies must assess their supply chain to identify, mitigate, and eliminate potential security risks.

The Global Security Verification standard is a program established by Intertek to help importers as well as suppliers assign their security measures based on international supply chain security requirements.

After 17 years of operational experience, CBP conducted the first ever review of CTPAT addressing evolving challenges and threats in the supply chain and released a new Minimum Security Criteria (MSC) on May 2019, incorporating requirements or recommendations related to cybersecurity, protection against agriculture, and the expansion of security technology.

Intertek incorporated these new MSC requirements, launching GSV 2.0 beginning of January 2020.

2. Objective and scope

In view of the escalating and evolving threat from global terrorism, governments and customs organizations around the world have implemented supply chain security standards to secure trade flows, protect against terrorist acts, and combat illegal trafficking.

In the process of enforcing and adhering to new international supply chain security standards, companies must assess their supply chain to identify, mitigate, and eliminate all potential security risks.

Intertek's Global Security Verification program GSV 2.0 integrates multiple global supply chain security initiatives, including CTPAT (Custom Trade Partnership Against Terrorism), PIP (Partners in Protection), and AEO (Authorized Economic Operators). Our mission is to partner with international buyers and suppliers to drive the development of a global security verification process, resulting in increased safety assurance, risk control, efficiency, and cost savings for all participants.

I. SCOPE AND BENEFITS

GSV 2.0 adopted CBP's new Minimum Security Criteria and other security supply chain initiatives:

Corporate Security
1. Security, vision, and responsibility (new)
2. Risk assessment
3. Business partner security
4. Cybersecurity (new)
Transportation Security
5. Conveyance and instruments of international traffic security
6. Seal security
7. Procedural security
8. Agricultural security (new)
People and physical security
9. Physical access controls
10. Physical security
11. Personnel security
12. Education, training, and awareness

3. Benefits

- Saving time and money by undergoing fewer security audits and thus reducing business disruptions
- Enhancing reputation with a world-recognized program that confirms compliance with global supply chain security criteria
- Enabling importers and suppliers to leverage efforts through a common industry platform and collaboration
- Engaging with a global security program, which covers best practice from CTPAT, PIP, and AEO

4. Summary of the Global Security Verification criteria

Intertek realigned previous GSV sections and will fully adopt the new CBP Minimum Security Criteria as GSV 2.0.

Section	Criteria
Corporate security	1. Security, vision, and responsibility (new) 2. Risk assessment 3. Business partner security 4. Cybersecurity (new)
Transportation security	5. Conveyance and instruments of international traffic security 6. Seal security 7. Procedural security 8. Agricultural Security (new)
People and physical security	9. Physical access controls 10. Physical security 11. Personnel security 12. Education, training, and awareness

5. Resources, references and definitions

Resources, references

- CTPAT new Minimum Security Criteria for Foreign Manufacturers 2019

Definitions[1]

- Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability and consequence. What determines the level of risk is how likely it is that a threat will happen.
- Business partner: A business partner is any individual or company whose actions may affect the chain of custody security of goods being imported to or exported from the USA via a CTPAT member's supply chain. A business partner may be any party that provides a service to fulfill a need within a company's international supply chain. These roles include all parties (both direct and indirect) involved in the purchase, document preparation, facilitation, handling, storage, and/or movement of cargo for, or on behalf of a CTPAT importer or exporter member. Two examples of indirect partners are subcontracted carriers and overseas consolidation warehouses – arranged for by an agent or logistics provider.

[1] Definitions as per CBP Foreign Manufacturers New MSC Booklet April 2019

- **Cybersecurity:** The activity or process that focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change, or destruction.
- **Instruments of international traffic:** Containers, flatbeds, unit load devices (ULDs), lift vans, cargo vans, shipping tanks, bins, skids, pallets, caul boards, cores for textile fabrics, or other specialized containers arriving (loaded or empty) in use or to be used in the shipment of merchandise in international trade.
- **Pest contamination:** Visible forms of animals, insects, other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi, soil, or water where such products are not the manifested cargo within instruments or international traffic (i.e. containers, unit load devices, etc.).
- **Sensitive positions:** This includes staff working directly with cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include but are not limited to: shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls.

CBP describes best practices as innovative security measures that exceed the CTPAT criteria and industry standards. For CTPAT purposes, a best practice must meet all five of the following requirements, all of which are subject to verification:

1. Senior management support
2. Innovative technology, process, or procedures
3. Documented process
4. Verifiable evidence
5. A regular system of checks, balances, and accountability (implementation)

II. CRITERIA IMPLEMENTATION GUIDANCE

The following section gives an explanation of the Global Security Verification Criteria (GSV 2.0) and provides guidance on what a facility needs to do to develop, document, and implement the criteria.

Corporate security

1. Security vision and responsibility

Intent: New category. A supply chain security program must become an integral part of the company's culture. There must be a high commitment and support from company's upper management.

Criteria	Implementation Indicators	Must/Should
Demonstrate commitment to supply chain security and the CTPAT program through a statement of support signed by a company's senior official, and displayed in appropriate company locations.	• Facility's statement of support signed by senior management. • Statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. • Display the statement of support in key areas of the company.	SHOULD
Incorporate representatives from all relevant departments into a cross-functional team.	• Supply chain security has a much broader scope than traditional security programs; it intertwines through many departments, along with security, such as human resources, information technology, and import/export offices.	SHOULD
The supply chain security program must be designed with, supported by, and implemented by an appropriate written review component. The purpose of this review component is to document that a system is in place whereby personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed.	• The review plan must be updated as needed based on pertinent changes in an organization's operations and level of risk. • The goal of a review for CTPAT purposes is to ensure that its employees are following the company's security procedures.	MUST

1. Security vision and responsibility

(Continued)

Criteria	Implementation Indicators	Must/Should
The Company's point(s) of contact (POC) to CTPAT must be knowledgeable about CTPAT program requirements. These individuals need to provide regular updates to upper management on issues related to the program, including the progress or outcomes of any audits, security related exercises, and CTPAT validations.	• Expectation: Designated POC to be a proactive individual who engages and is responsive to his or her supply chain security specialist.	MUST

Corporate security

2. Risk assessment

Intent: The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for members to assess existing and potential exposure to these evolving threats. When determining risk within their supply chains, members must consider various factors such as the business model, geographic location and other aspects that may be unique to a specific supply chain.

Criteria	Implementation Indicators	Must/Should
CTPAT members must conduct and document the amount of risk in their supply chains. CTPAT members must conduct an overall risk assessment (RA) to identify where security vulnerabilities may exist. The risk assessment must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities.	• The overall risk assessment (RA) is made up of two key parts. The first part is a self-assessment of the member's supply chain security practices, procedures, and policies within the facilities that it controls to verify its adherence to CTPAT's minimum-security criteria, and an overall management review of how it is managing risk. • The second part of the RA is the international risk assessment. This portion of the RA includes the identification of geographical threat(s) based on the member's business model and role in the supply chain. • CTPAT 5 Risk Assessment Document can be found here: https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf	MUST
The international portion of the risk assessment should document or map the movement of the member's cargo throughout its supply chain from the point of origin to the importer's distribution center. The mapping should include all business partners involved both directly and indirectly in the exportation/movement of the goods.	• Supply chain security has a much broader scope than traditional security programs; it intertwines through many departments, along with security, such as human resources, information technology, and import/export offices.	SHOULD

2. Risk assessment

(Continued)

Criteria	Implementation Indicators	Must/Should
Review risk assessment annually or more frequently as risk factors dictate.	• Circumstances that may require a risk assessment to be reviewed more frequently than once a year include an increased threat level from a specific country, periods of heightened alert, following a security breach or incident, changes in business partners, and/or changes in corporate structure/ ownership such as mergers and acquisitions etc.	MUST
CTPAT members should have written procedures addressing crisis management, business continuity, security recovery plans, and business resumption.	• A crisis may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the member operates or sources from, contingency plans may include additional security notifications or support and how to recover what was destroyed or stolen and get back to normal operating conditions.	SHOULD

Corporate security

3. Business partner security

Intent: CTPAT members engage with a variety of business partners, both domestically and internationally. For those business partners that directly handle cargo and/or import/export documentation, it is crucial for the member to ensure that these business partners have appropriate security measures in place to secure the goods through the international supply chain.

Criteria	Implementation Indicators	Must/Should
CTPAT members must have a written, risk-based process for screening new business partners and for monitoring current partners. A factor that members should include in this process is checks on activity related to money laundering and terrorist funding.	• Examples of some of the vetting elements that can help determine if a company is legitimate: - Verifying the company's business address and how long they have been at that address; - Conducting research on the internet on both the company and its principals; - Checking business references; and - Requesting a credit report. • How in-depth to make the screening depends on the level of risk in the supply chain.	MUST
The business partner screening process must take into account whether a partner is a CTPAT member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA). Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners, and members must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification.	• Business partners' CTPAT certification may be ascertained via the CTPAT portal's status verification Interface system. • If the business partner certification is from a foreign AEO program under an MRA with the United States, the foreign AEO certification will include the security component. members may visit the foreign customs administration's website where the names of the AEOs of that customs administration are listed, or request the certification directly from their business partners. • The company must have written or electronic confirmation of its partners' compliance with CTPAT or CTPAT-equivalent security criteria (e.g. contract language, a letter of commitment signed at the management level or above, signed acknowledgement of receiving the company's CTPAT participation announcement.)	MUST

3. Business partner security
(Continued)

Criteria	Implementation Indicators	Must/Should
Where a CTPAT member outsources or contracts elements of its supply chain, the member must exercise due diligence to ensure these business partners have security measures in place that meet or exceed CTPAT's MSC.	• Based on risk, the company may conduct an onsite audit at the facility, hire a contractor/ service provider to conduct an onsite audit or use a security questionnaire. • More details may be required from companies located in high-risk areas.	MUST
If weaknesses are identified during business partners' security assessments, they must be addressed as soon as possible, and corrections must be implemented in a timely manner. Members must confirm that deficiencies have been mitigated via documentary evidence.	• Based on the level of risk involved and the importance of the weakness found, some issues may require immediate attention. • Some examples of documentary evidence may include copies of contracts for additional security guards, photographs taken of a newly installed security camera or intrusion alarm, or copies of inspection checklists, etc.	MUST
To ensure their business partners continue to comply with CTPAT's security criteria, members should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate.	• Periodically reviewing business partners' security assessments is important to ensure that a strong security program is still in place and operating properly. • Based on the member's risk assessment process. • Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country, changes in source location, and new critical business partners (those that actually handle the cargo, provide security to a facility, etc.)	MUST
For inbound shipments to the United States, if a member subcontracts transportation services to another highway carrier, the member must use a CTPAT certified highway carrier or a highway carrier that works directly for the member as delineated through a written contract. The contract must stipulate adherence to all Minimum Security Criteria (MSC) requirements.	• The carrier should provide a list of subcontracted carriers and drivers to the facilities where it picks up and delivers cargo. Any changes to the subcontractor list should be immediately conveyed to relevant partners. • When reviewing service providers for compliance, the member should verify that the company subcontracted is actually the company transporting the loads—and has not further subcontracted loads without approval.	MUST

3. Business partner security

(Continued)

Criteria	Implementation Indicators	Must/Should
CTPAT members should have a documented social compliance program in place that, at a minimum, addresses how the company ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced imprisoned, indentured, or indentured child labor.	• The company should have a documented social compliance program that ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of forced, imprisoned, indentured, or indentured child labor.	SHOULD

Corporate security

4. Cybersecurity

Intent: New category. Cybersecurity is the key to safeguarding precious assets: intellectual property, customer information, financial data, and employee records, among others. With increased connectivity to the internet comes the risk of a breach of a company's information systems. Measures to secure a company's information technology (IT) and data are crucial.

Criteria	Implementation Indicators	Must/Should
CTPAT members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual cybersecurity criteria.	• Members are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/standards.	MUST
To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in members' computer systems. Members must ensure that their security software is current and receives regular security updates.	• Members must have policies and procedures to prevent attacks via social engineering. • If a data breach occurs or other unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.	MUST
CTPAT members utilizing network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.	• Scheduling vulnerability scans. • A vulnerability scan (VS) identifies openings on your computers (open ports and IP addresses), their operating systems, and software through which a hacker could gain access to the company's IT system. • The frequency of the testing will depend on various factors to include the company's business model and level of risk.	MUST
Cybersecurity policies should address how a member shares information on cybersecurity threats with the government and other business partners.	Members are encouraged to share information on cybersecurity threats with the government and business partners within their supply chain.	SHOULD

4. Cybersecurity
(Continued)

Criteria	Implementation Indicators	Must/Should
A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.		MUST
Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.	An example of a circumstance that would dictate a policy update sooner than annually is a cyber attack.	MUST
User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.		MUST
Individuals with access to information technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be safeguarded.	Complex login passwords or passphrases, biometric technologies, and electronic ID cards are three different types of authentication processes.	MUST
Members that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.	VPNs are not the only choice to protect remote access to a network. Multi-factor authentication (MFA) is another method.	MUST

4. Cybersecurity

(Continued)

Criteria	Implementation Indicators	Must/Should
If members allow employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.	Personal devices include storage media like CDs, DVDs, and USB flash drives. Care will be used if employees are allowed to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network.	MUST
Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.	Members may want to have a policy that requires product key labels and certificates of authenticity to be kept when new media is purchased.	SHOULD
Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.	• Daily backups may be needed because of the effect that data loss may have on multiple personnel, if production or shared servers are compromised/lose data. • Back up policy and system	SHOULD
All media, hardware, or other IT equipment that contains sensitive information regarding the import/export process must be accounted for through regular inventories. When disposed, they must be properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines.	Members may want to consult NIST standards for sanitation and destruction of IT equipment and media.	MUST

Transportation security

5. Conveyance and instruments of international traffic security

Intent: This criteria covers security measures designed to prevent, detect, and/or deter the altering of IIT structures or surreptitious entry into them, which could allow the introduction of unauthorized material to persons.

Criteria	Implementation Indicators	Must/Should
Conveyances and instruments of international traffic (IIT) must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an instruments of international traffic or (as applicable) allow the seal/doors to be compromised.	The secure storage of conveyances and instruments of international traffic (both empty and full) is important to guard against unauthorized access.	MUST
The CTPAT inspection process must have written procedures for both security and agricultural inspections.	It is imperative that members conduct inspections of conveyances and instruments of international traffic to look for visible pests and serious structural deficiencies. Likewise, the prevention of pest contamination via conveyances and IIT is of paramount concern, so an agricultural component has been added to the security inspection process.	MUST
Prior to loading/stuffing/packing, all conveyances and empty instruments of international traffic must undergo CTPAT approved security and agricultural inspections to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests. A seven-point inspection on all empty containers and unit load devices (ULD), and an eight-point inspection on all empty refrigerated containers and ULDs must be conducted prior to loading/stuffing.	Prior to loading/stuffing/packing, all conveyances and empty instruments of international traffic must undergo CTPAT approved security and agricultural inspections to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests. In addition to the seven-point inspection, add key checkpoints such as cleanliness of the container, if is it possible to visually identify any contaminant, and confirm WPM marking if applicable.	MUST

5. Conveyance and instruments of international traffic security

(Continued)

Criteria	Implementation Indicators	Must/Should
Conveyances and instruments of international traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.	Consider using containers/trailers with tamper resistant hinges. Members may also place protective plates or pins on at least two of the hinges of the doors and/or place adhesive seal/ tape over at least one hinge on each side.	MUST
The inspection of all conveyances and empty instruments of international traffic should be recorded on a checklist. If the inspections are supervised, the supervisor should also sign the checklist. The completed container/instruments of international traffic inspection sheet should be part of the shipping documentation packet. The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.	The following elements should be documented on the checklist: • Container/trailer/instruments of international traffic number; • Date of inspection; • Time of inspection; • Name of employee conducting the inspection; and • Specific areas of the instruments of international traffic that were inspected.	SHOULD
All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.		SHOULD
If visible pest contamination is found during the conveyance/Instruments of international traffic inspection, washing/vacuuming must be carried out to remove such contamination. Documentation must be retained for one year to demonstrate compliance with these inspection requirements.	Keeping records on the types of contaminants found, where they were found (conveyance location), and how the pest contamination was eliminated, are helpful actions that may assist members in preventing future pest contamination.	MUST

5. Conveyance and instruments of international traffic security
(Continued)

Criteria	Implementation Indicators	Must/Should
Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of international traffic inspections. The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border.	• As a best practice, supervisors can hide an item (like a toy or colored box) in the conveyance to determine if the field test screener/ conveyance operator finds it. • Supervisory personnel could be a security manager, held accountable to senior management for security, or other designated management personnel.	SHOULD
CTPAT members should work with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.	Review procedure if there is responsible person/s to track transportation services at point of origin to destination point.	SHOULD
Shippers should have access to their carrier's GPS fleet monitoring system, so they may track the movement of their shipments.	Review procedure and ask to verify request to see a track and trace report of a shipment.	SHOULD
For land border shipments that are in proximity to the United States border, a "no-stop" policy should be implemented with regard to unscheduled stops.	Cargo at rest is cargo at risk. Scheduled stops would not be covered by this policy, but would have to be considered in an overall tracking and monitoring procedure.	SHOULD

5. Conveyance and instruments of international traffic security

(Continued)

Criteria	Implementation Indicators	Must/Should
In areas of high risk and immediately prior to arrival at the border crossing, CTPAT members should incorporate a "last chance" verification process for U.S. bound shipments for checking conveyances/Instruments of International Traffic for signs of tampering to include visual inspections of conveyances and the VVTT seal verification process.	Properly trained individuals should conduct the inspections. V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.	SHOULD
If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the member must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate.	The company must have documented procedure to immediately alert any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate.	MUST

Transportation security

6. Seal security

Intent: Comprehensive written seal policy that addresses all aspects of seal security. (Using correct seals as per CTPAT requirements, properly placing a seal on an IIT, and verifying that the seal has been affixed properly.)

Criteria	Implementation Indicators	Must/Should
CTPAT members must have detailed, written high security seal procedures that describe how seals are issued and controlled at the facility and during transit. Procedures must provide the steps to take if a seal is found to be altered, tampered with, or has the incorrect seal number to include documentation of the event, communication protocols to partners, and investigation of the incident. The findings from the investigation must be documented, and any corrective actions must be implemented as quickly as possible. These written procedures must be maintained at the local, operating level so that they are easily accessible. Procedures must be reviewed at least once a year and updated as necessary.	Written seal controls must include the following elements: Controlling access to seals: • Management restricted to authorized personnel. • Secure storage • Recording the receipt of new seals. • Issuance of seals recorded in log. • Track seals via the log. • Only trained, authorized personnel may affix seals to (IIT). Controlling seals in transit: • When picking up sealed IIT verify the seal has no signs of tampering. • Confirm the seal number with shipping documents. Seals broken in transit: • If load examined--record replacement seal number. • The driver must immediately notify dispatch when a seal is broken. • The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number. • The shipper must note the replacement seal number Seal discrepancies: • Hold any seal discovered to be altered or tampered. • Investigate the discrepancy. • As applicable, report compromised seals to CBP and the appropriate foreign government.	MUST

6. Seal security
(Continued)

Criteria	Implementation Indicators	Must/Should
CTPAT members that maintain seal inventories must be able to document the high security seals they use either meet or exceed the most current ISO 17712 standard.	• The high security seal used must be placed on the secure cam position, if available, instead of the right door handle. • The seal must be placed at the bottom of the center most vertical bar of the right container door. Alternatively, the seal could be placed on the center most/left hand locking handle on the right container door if the secure cam position is not available. • If a bolt seal is being used, it is recommended that the bolt seal be placed with the barrel portion or insert facing upward with the barrel portion above the hasp.	MUST
CTPAT members (that maintain seal inventories) must be able to document the high security seals they use either meet or exceed the most current ISO 17712 standard.	Copy of a laboratory testing certificate that demonstrates compliance with the ISO high security seal standard.	MUST
If a member maintains an inventory of seals, company management or a security supervisor must conduct audits of seals that includes periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented. As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on conveyances and instruments of international traffic.	• Seal policy and procedures • Audits	MUST

6. Seal security

(Continued)

Criteria	Implementation Indicators	Must/Should
CTPAT's seal verification process must be followed to ensure all high security seals (bolt/cable) have been affixed properly to instruments of international traffic, and are operating as designed. The procedure is known as the VVTT process: V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.	• When applying cable seals, it is needed to envelop the rectangular hardware base of the vertical bars in order to eliminate any upward or downward movement of the seal. • Once the seal is applied, make sure that all slack has been removed from both sides of the cable. • The VVTT process for cable seals needs to ensure the cables are taut. Once it has been properly applied, tug and pull the cable in order to determine if there is any cable slippage within the locking body.	MUST

Transportation security

7. Procedural security

Intent: Procedural Security comprehends many aspects of the import-export process, documentation, and cargo storage and handling requirements. CTPAT members must ensure integrity and security of processes relevant to transportation, handling and storage of cargo in the supply chain.

Criteria	Implementation Indicators	Must/Should
When cargo is staged overnight, or for an extended period of time, measures must be taken to secure the cargo from unauthorized access	When cargo is staged overnight, or for an extended period of time, measures must be taken to secure the cargo from unauthorized access.	MUST
Cargo staging areas and the immediate surrounding areas must be inspected on a regular basis to ensure these areas remain free of visible pest contamination.	Preventative measures such as the use of baits, traps, or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas.	MUST
The loading/stuffing of cargo into containers/ IIT should be supervised by a security officer/ manager or other designated personnel.	Verify job description, responsibilities, and training records of designated person or responsible person for loading and departure of containers area.	SHOULD
As documented evidence of the properly installed seal, digital photographs should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.	Photographic evidence may include pictures taken at the point of stuffing to document evidence of the cargo markings, the loading process, the location where the seal was placed, and properly installed seal.	SHOULD
Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time	Review a written procedure how shipping documents are prepared and that these documents are completely legible and accurate.	MUST
If paper is used, forms and other import/ export related documentation should be secured to prevent unauthorized use.	Measures, such as using a locked filing cabinet, can be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation.	SHOULD

7. Procedural security

(Continued)

Criteria	Implementation Indicators	Must/Should
The shipper or its agent must ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, and carriers must exercise due diligence to ensure these documents are accurate. BOLs and manifests must be filed with U.S. Customs and Border Protection (CBP) in a timely manner. BOL information filed with CBP must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States. The weight and piece count must be accurate.	• When picking up sealed instruments of international traffic, carriers may rely on the information provided in the shipper's shipping instructions. • Requiring the seal number to be electronically printed on the bill of lading (BOL) or other export documents helps guard against changing the seal and altering the pertinent document(s) to match the new seal number. • For certain supply chains, goods may be examined in transit, by a foreign Customs authority, or by CBP. • Once the seal is broken by the government, there needs to be a process to record the new seal number applied to the IIT after examination. In some cases, this may be handwritten.	MUST
CTPAT members must have written procedures for reporting an incident to include a description of the facility's internal escalation process. A notification protocol must be in place to report any suspicious activities or security incidents that may affect the security of the member's supply chain. As applicable, the member must report an incident to its SCSS, the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain. Notifications to CBP should be made as soon as feasibly possible and in advance of any conveyance or IIT crossing the border.	Examples of incidents warranting notification to CBP include (but are not limited to) the following: • Discovery of tampering with a container/IIT or high security seal; • Discovery of a hidden compartment in a conveyance or IIT; • An unaccounted new seal has been applied to an IIT; • Smuggling of contraband to include people; stowaways; • Unauthorized entry into conveyances, locomotives, vessels, or aircraft carriers; • Extortion, payments for protection, threats, and/or intimidation; • Unauthorized use of a business entity identifier (i.e., Importer of Record (IOR) number, Standard Carrier Alpha Code (SCAC), etc.).	MUST

7. Procedural security
(Continued)

Criteria	Implementation Indicators	Must/Should
Procedures must be in place to identify, challenge, and address unauthorized/ unidentified persons. Personnel must know the protocol to challenge an unknown/ unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.	• The company should have positive identification process for recording all vendors and repair personnel and should have a written procedure to challenge, identify, and remove unauthorized/ unidentified persons. • Personnel should be properly trained.	MUST
CTPAT members should set up a mechanism to report security related issues anonymously. When an allegation is received, it should be investigated, and if applicable, corrective actions should be taken.	• Internal problems such as theft, fraud, and internal conspiracies may be reported more readily if the reporting party knows the concern may be reported anonymously. • Members can set up a hotline program or similar mechanism that allows people to remain anonymous if they fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each reported item was investigated and that corrective actions were taken.	SHOULD
All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate.		MUST
Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.		SHOULD

7. Procedural security

(Continued)

Criteria	Implementation Indicators	Must/Should
Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.		SHOULD
Seal numbers should be electronically printed on the bill of lading or other shipping documents.		SHOULD
Following a significant security incident, Members must initiate a post-incident analysis immediately after becoming aware of the incident and in order to determine where the supply chain may have been compromised. NEW	• A security incident is a breach in which security measures have been circumvented, eluded, or violated, and have resulted or will result in a criminal act. Security incidents include acts of terrorism, smuggling (narcotics, human, etc.), and the presence of stowaways. • This analysis must not impede/interfere with any known investigations conducted by a government law enforcement agency. • The company's post-incident analysis findings must be documented, completed as soon as feasibly possible, and, if allowed by law enforcement authorities, made available to the SCSS upon request.	MUST

Transportation security

8. Agricultural security

Intent: New category. Agriculture is the largest industry and employment sector in the United States, an industry threatened by the introduction of foreign animal and plant contaminants such as soil, manure, seeds, and plant and animal material which may harbor invasive and destructive pests and diseases. Eliminating contaminants in all conveyances and all types of cargo may decrease cargo holds, delays and commodity returns or treatments.

Criteria	Implementation Indicators	Must/Should
CTPAT members must have written procedures designed to prevent visible pest contamination to include compliance with wood packaging materials regulations. Visible pest prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).	• The company must have documented written procedures for wood packaging materials. • There should be visible pest preventions flowed throughout the supply chain and adhered to. • There should be compliance with IIPC - ISPM 15	MUST

People and physical security

9. Physical security

Intent: Physical security criteria provides a number of deterrents/obstacles that will help prevent unwarranted access to cargo, sensitive equipment, and/or information, and Members should employ these security measures throughout their supply chains.

Criteria	Implementation Indicators	Must/Should
All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.		MUST
Perimeter fencing should enclose the areas around cargo handling and storage facilities. If a facility handles cargo, interior fencing should be used to secure cargo and cargo handling areas. Based on risk, additional interior fencing should segregate various types of cargo such as domestic, international, high value, and/or hazardous materials. Fencing should be regularly inspected for integrity and damage by designated personnel. If damage is found in the fencing, repairs should be made as soon as possible.	Other acceptable barriers may be used instead of fencing, such as a dividing wall or natural features that are impenetrable or otherwise impede access such as a steep cliff or dense thickets.	SHOULD
Gates where vehicles and/or personnel enter or exit (as well as other points of egress) must be manned or monitored. Individuals and vehicles may be subject to search in accordance with local and labor laws.	It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated.	MUST
Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.	In order to minimize the risk of cargo being stolen or compromised by allowing for contraband commingled with cargo to have an easier pathway in/out, locate parking areas outside of fenced and/or operational areas - or at least at substantial distances from cargo handling and storage areas.	SHOULD
Adequate lighting must be provided inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas	Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.	MUST

9. Physical security
(Continued)

Criteria	Implementation Indicators	Must/Should
Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas.	• Security technology used to secure sensitive areas/access points includes alarms, access control devices, and video surveillance systems such as closed caption television cameras (CCTVs). • Sensitive areas, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for instruments of international traffic (IIT), areas where IIT are inspected, and seal storage areas.	SHOULD
Members who rely on security technology for physical security must have written policies and procedures governing the use, maintenance, and protection of this technology. Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.	Security technology needs to be tested on a regular basis to ensure it is working properly.	MUST
CTPAT members should utilize licensed/certified resources when considering the design and installation of security technology.	Seeking qualified guidance will help a buyer select the right technology options for their needs and budget.	SHOULD
All security technology infrastructure must be physically secured from unauthorized access.	Security technology infrastructure includes computers, security software, electronic control panels, video surveillance or closed circuit television cameras, power and hard drive components for cameras, as well as recordings.	MUST

9. Physical security

(Continued)

Criteria	Implementation Indicators	Must/Should
Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.	• An alternative power source may be an auxiliary power generation source or backup batteries. • Backup power generators may also be used for other critical systems such as lighting.	SHOULD
If camera systems are deployed, cameras should monitor a facility's premises and sensitive areas to deter unauthorized access. Alarms should be used to alert a company to unauthorized access into sensitive areas.	Sensitive areas, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for instruments of international traffic (IIT), areas where IIT are inspected, and seal storage areas.	SHOULD
If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to the import/export process. Cameras should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis.	Specific areas (based on risk) of security focus would include cargo handling and storage; shipping/receiving; cargo loading process, sealing process; conveyance arrival/exit; IT servers; container inspections (security and agricultural); seal storage; and any other areas that pertain to securing international shipments.	MUST
If camera systems are deployed, cameras should have an alarm/notification feature, which would signal a "failure to operate/record" condition.	The failure to operate feature can result in an electronic notification sent to predesignated person(s) notifying them that the device requires immediate attention.	SHOULD

9. Physical security

(Continued)

Criteria	Implementation Indicators	Must/Should
If camera systems are deployed, periodic, random reviews of the camera footage must be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with law. Results of the reviews must be summarized in writing to include any corrective actions taken. The results must be maintained for a sufficient time for audit purposes.	Focus the random review of the footage on the physical chain of custody to ensure the shipment remained secure and all security protocols were followed. Some examples of processes that may be reviewed are the following: • Cargo handling activities; • Container inspections; • The loading process; • Sealing process; • Conveyance arrival/exit; and • Cargo departure, etc.	MUST
If cameras are being used, recordings of footage covering key import/export processes should be maintained for a sufficient time for a monitored shipment to allow an investigation to be completed.	All video surveillance recording must be continuous or motion detection activated, 24 hours a day, 7 days a week. Recorded surveillance images must be stored for at least 30 days or according to client's requirement whichever if longer. Some experts recommend allotting at least 14 days after the shipment being monitored has arrived at the first point of distribution, where the container is first opened after clearing Customs..	SHOULD

People and physical security

10. Physical access controls

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

Criteria	Implementation Indicators	Must/Should
CTPAT members must have written procedures governing how identification badges and access devices are granted, changed, and removed. Where applicable, a personnel identification system must be in place for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties. Removal of access devices must take place upon the employee's separation from the company.	• Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes, and keys. • When employees are separated from a company, the use of exit checklists help ensure that all access devices have been returned and/or deactivated. • For smaller companies, where personnel know each other, no identification system is required. • Generally, for a company with more than 50 employees, an identification system is required.	MUST
Visitors, vendors, and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors should be escorted. In addition, all visitors and service providers should be issued temporary identification. If temporary identification is used, it must be visibly displayed at all times during the visit.	The registration log must include the following: • Date of the visit; • Visitor's name; • Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure.	

10. Physical access controls

(Continued)

Criteria	Implementation Indicators	Must/Should
Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government-issued photo identification to the facility employee granting access to verify their identity. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load.	Procedure for drivers identification verification.	MUST
A cargo pickup log must be kept to register drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it.	The cargo pickup log should have the following items recorded: • Driver's name; • Date and time of arrival; • Employer; • Truck number; • Trailer number; • Time of departure; • The seal number affixed to the shipment at the time of departure.	MUST
Prior to arrival, the carrier should notify the facility of the estimated time of arrival for the scheduled pick up, the name of the driver, and truck number. Where operationally feasible, CTPAT Members should allow deliveries and pickups by appointment only.	When a carrier has regular drivers that pick up goods from a certain facility, a good practice is for the facility to maintain a list of the drivers with their pictures.	SHOULD

10. Physical access controls

(Continued)

Criteria	Implementation Indicators	Must/Should
Arriving packages and mail should be periodically screened for contraband before being admitted.	• Documented procedures should be implemented to periodically screen arriving packages and mail prior to distribution. • Examples of such contraband include, but are not limited to, explosives, illegal drugs, and currency.	SHOULD
If security guards are used, work instructions for security guards must be contained in written policies and procedures. Management must periodically verify compliance and appropriateness with these procedures through audits and policy reviews.	Work instructions in writing.	MUST

People and physical security

11. Personnel security

Intent: A company's human resource force is one of its most critical security assets, but it may also be one of its weakest security links. The criteria in its category focus on issues such as employee screening and pre-employment verifications. Members must exercise due diligence to verify that employees filling sensitive positions are reliable and trustworthy.

Criteria	Implementation Indicators	Must/Should
Application information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law.	CTPAT is aware that labor and privacy laws in certain countries may not allow all of the application information to be verified. Nevertheless, it is expected to verify application information when able to do so.	MUST
In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors. Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position. Employee background screening should include verification of the employee's identity and criminal history that encompass city, state, provincial, and country databases. CTPAT members and their business partners should factor in the results of background checks, as permitted by local statutes, in making hiring decisions. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, it may warrant more in-depth investigations.	• Employee background checks • Hiring policies	SHOULD
CTPAT Members must have an Employee Code of Conduct that includes expectations and defines acceptable behaviors. Penalties and disciplinary procedures must be included in the Code of Conduct. Employees/contractors must acknowledge that they have read and understood the Code of Conduct by signing it, and this acknowledgement must be kept in the employee's file for documentation. **NEW**	• A Code of Conduct helps protect company's business and informs employees of expectations. • Its purpose is to develop and maintain a standard of conduct that is acceptable to the company. • It helps companies develop a professional image and establish a strong ethical culture. • Even a small company needs to have a Code of Conduct; however, it does not need to be elaborate in design or contain complex information.	MUST

People and physical security

12. Education, training, and awareness

Intent: One of the key aspects to maintaining a security program is training. Educating employees on what threats are is crucial. When employees understand why security procedures are in place, they are much more likely to adhere to them.

Criteria	Implementation Indicators	Must/Should
Members must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. The training program must be comprehensive and cover all of CTPAT's security requirements. Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds. One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required based on their functions and position, on a regular basis, and newly hired employees must receive this training as part of their orientation/job skills training.	Members must retain evidence of training such as training logs, sign in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.	MUST
Drivers and other personnel that conduct security and agricultural inspections of empty conveyances and instruments of international traffic (IIT) must be trained to inspect their conveyances/IIT for both security and agricultural purposes. Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures.	Inspection training must include the following topics: • Signs of hidden compartments; • Concealed contraband in naturally occurring compartments; and • Signs of pest contamination.	MUST

12. Education, training, and awareness

(Continued)

Criteria	Implementation Indicators	Must/Should
CTPAT members should have measures in place to verify that the training provided met all training objectives.	Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that the member may implement to determine the effectiveness of the training.	SHOULD
As applicable based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.	Quality training is important to lessen vulnerability to cyber attacks. A robust cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.	MUST
Personnel operating and managing security technology systems must have received training in their operation and maintenance. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable.	Training records and content	MUST
Personnel must be trained on how to report security incidents and suspicious activities.	Training on how to report an incident can be included in the overall security training. Specialized training modules (based on job duties) may have more detailed training on reporting procedures to include specifics on the process - what to report, to whom, how to report it, and what to do next, after the report.	MUST

Appendix

Country	Intertek Country Supply Chain Security Risk Index
Argentina	HIGH
Australia	LOW
Austria	LOW
Bahrain	HIGH
Bangladesh	HIGH
Belgium	LOW
Brazil	MEDIUM
Brunei	LOW
Bulgaria	MEDIUM
Cambodia	HIGH
Canada	LOW
Chile	HIGH
China	MEDIUM
Costa Rica	MEDIUM
Croatia	MEDIUM
Cyprus	MEDIUM
Czech Republic	MEDIUM
Denmark	LOW
Dominican Republic	MEDIUM
Ecuador	MEDIUM
Egypt	HIGH
El Salvador	MEDIUM
Ethiopia	MEDIUM
Fiji	LOW
Finland	LOW
France	LOW
Germany	LOW
Ghana	MEDIUM
Greece	MEDIUM
Guatemala	HIGH
Haiti	HIGH
Honduras	HIGH
Hungary	LOW
Iceland	LOW
India	HIGH
Indonesia	HIGH
Ireland	LOW
Israel	HIGH
Italy	LOW
Japan	LOW
Jordan	HIGH
Kenya	MEDIUM
Kuwait	HIGH
Laos	MEDIUM
Latvia	LOW
Lebanon	HIGH
Lesotho	MEDIUM
Madagascar	HIGH
Malaysia	HIGH
Mauritius	LOW
Mexico	HIGH
Morocco	HIGH
Myanmar	HIGH
Netherlands	LOW
New Zealand	LOW
Norway	LOW
Oman	HIGH
Pakistan	HIGH
Panama	MEDIUM
Peru	HIGH
Philippines	HIGH
Poland	MEDIUM
Portugal	LOW
Romania	MEDIUM
Russia	HIGH
Saudi Arabia	HIGH
Serbia	MEDIUM
Singapore	LOW
Slovakia	MEDIUM
South Africa	MEDIUM
South Korea	LOW
Spain	LOW
Sri Lanka	MEDIUM
Sweden	LOW
Switzerland	LOW
Taiwan	LOW
Thailand	MEDIUM
Tunisia	HIGH
Turkey	HIGH
Ukraine	MEDIUM
United Arab Emirates	HIGH
United Kingdom	LOW
USA	LOW
Venezuela	HIGH
Vietnam	MEDIUM

The “Intertek Country Supply Chain Security Risk Index” predicts the supply chain security risk associated with a number of parameters in each country including but not limited to:

1. Practice for cargo logistics
2. Clearance and customs process
3. Political and economic condition
4. Historical country performance in security verifications for the last 10 years.

III. INTERTEK'S SUPPLIER QUALIFICATION PROGRAMMES

Your guide in all fields:

Intertek audit services

Creating better suppliers

Our audit services facilitate continuous improvement, producing better suppliers.

- All standards are aligned with industry best practices.
- All audit services are based on the continuous improvement approach.
- Suppliers are motivated through industry, country, and global benchmarking to improve and evolve.
- Our programs are widely adopted or accepted by many global retailers and brands.
- Good performance will be recognized through achievement award or record participation.

Identifying the needs and areas for improvement, the current audit programs are divided into the following groups:

Social	Environment		Quality		Security
WORKPLACE CONDITIONS ASSESSMENT	THINK GREEN INITIATIVE	ENVIRONMENTAL CHEMICAL MANAGEMENT	SUPPLIER QUALIFICATION PROGRAM	MILL QUALIFICATION PROGRAM	GLOBAL SECURITY VERIFICATION

Second Party Audits

More qualification

Undertaking our audit services,which also work as qualification programs, allows you to increase your facility's compliance.

It enables you to map the compliance risk in your supply chain through the effective use of reports and charts in order to keep track of supplier performance against industry, country, and global benchmarks.

Continuous improvement

Intertek supplier risk management services are not the traditional pass or fail audit programs. Instead, continuous improvement is possible with constant feedback and monitoring of results. The outcomes are measurable through statistics.

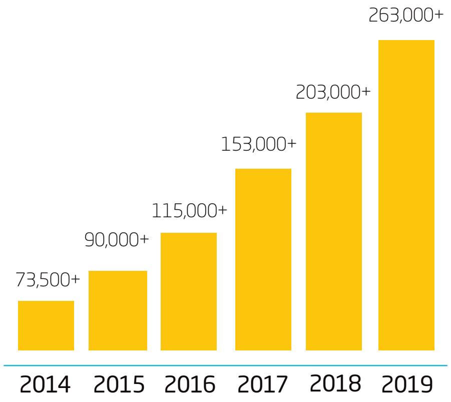
Intertek also provides audit services against second-party customer-specific programs or requirements, and training and capacity-building options for supplier performance improvement.

Widely accredited

We are one of the largest service providers for audits under industry-specific accreditation schemes:

- British Retail Consortium (BRC)
- amfori Business Social Compliance Initiative (amfori BSCI)
- Responsible Business Alliance (RBA)
- Initiative Clause Sociale (ICS)
- Social Accountability International (SA8000)
- Supplier Ethical Data Exchange (Sedex)
- Worldwide Responsible Accredited Production (WRAP)

On-site verifications performed



With more than 263,000 participating facilities, Intertek's range of supplier audit services represents the world's largest community of verified suppliers.

Intertek audit services:

The world's largest community of verified suppliers

Data mining

Intertek audit services create the world's largest community of suppliers and make data mining of supplier performance possible. Detailed reports enable suppliers to know their strengths and challenges.

Buyers can better manage their suppliers and make more informed buying decisions.

Benchmarking

Benchmarking of supplier performance against country, industry or global averages provides suggestions for targeted improvements, based on performance and challenging factors.

Report sharing

Suppliers and facilities can easily share audit reports with their clients. Intertek's reports are recognized by most of the world's leading buyers.

This can help reduce audit fatigue and business disruption, as suppliers and facilities do not have to complete audits for different buyers.

Achievement award

Our programs reward suppliers who fulfill assessment criteria with an achievement award or record of participation.

The awarded suppliers or facilities can use the program logo and award as a valuable marketing tool to showcase their performance to buyers.

Intertek is a leading Total Quality Assurance provider to industries worldwide. Our network of more than 1,000 laboratories and offices and over 44,000 people in more than 100 countries, delivers innovative and bespoke Assurance, Testing, Inspection and Certification solutions for our customers' operations and supply chains. Intertek Total Quality Assurance expertise, delivered consistently with precision, pace and passion, enabling our customers to power ahead safely.

FOR MORE INFORMATION

Intertek
900 Chelmsford St
Lowell, MA
USA
01851

☎ +1 800 810 1995

✉ business.assurance@intertek.com

intertek.com/business-assurance/supplier-management/security-verification

intertek
Total Quality. Assured.