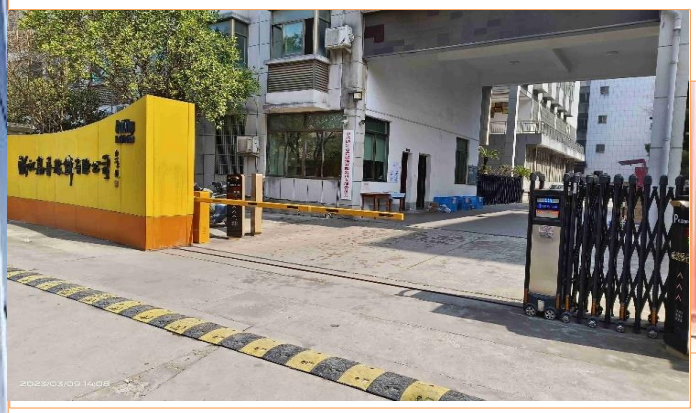
Audit Date:	Mar.9,2023
Audit Type:	Initial Audit

ZHEJIANG GOLDTOP HAT & FASHION CO.,LTD

SECURITY ASSESSMENT



AUDIT SUMMARY

ZHEJIANG GOLDTOP HAT & FASHION CO.,LTD was located at 5, The 2nd Danchen RD., Beiyuan Industrial Zone, Yiwu City, Zhejiang Province.The factory established the C-TPAT manual and relevant C-TPAT procedures.
The factory had 2 security guards to conduct secuity issues.
During the audit, the factory management showed a cooperative attitude to this audit and agreed auditor to conduct on site audit of whole area and interview with relevant employees, reviewed the all relevant records and documents. The management stated that they would take action to close the findings during audit as soon as possible.

SITE PROFILE

Basic Information

Supplier Name	ZHEJIANG GOLDTOP HAT & FASHION CO.,LTD			
Facility Address	5, The 2nd Danchen RD., Beiyuan Industrial Zone, Yiwu City, Zhejiang Province			
City	Yiwu			
State / Province	Zhejiang			
Country	China			
Postal Code	322000			
Supplier's Telephone No.	18957959905			
Supplier's Fax No.	0579-85260966			
Supplier's E-mail Address	gp6668@hatoem.com			
Supplier's Web-site	Nil			
C-TPAT Member		YES	X	NO
Business Partner to C-TPAT member		YES	X	NO
Month/Year Started Operations	08/2004			
Other Location 1	Nil			
Other Location 2	Nil			
Other Location 3	Nil			

Supplier Contacts

President	Mr.Zhu Zhihui	Email: Nil
Plant Manager	Mr. Tong Yuanqing	Email: Nil
Quality Manager	Ms. Yan Xinjiao	Email: gp5250@hatoem.com
Safety Representative	Mr. Yang Hui	Email: gp6668@hatoem.com
HR Manager	Mr. Yang Hui	Email: gp6668@hatoem.com
Housing Manager	Mr. Xu Zhuxing	Email: Nil
Security Manager	Mr. Xu Zhuxing	Email: Nil
Other - *Type Title here.*	Nil	
Other - *Type Title here.*	Nil	

Background Information

Product / Service Category(s)	Hats
Operation Process(es)	Raw materials-cutting-complexing-sewing-ironing-inspecting-packing

Annual Sales (USD)	190000000
Capacity/Year (Units)	10000000 piece
Main Language of Employees	Chinese
Language of Management	Chinese
Business Nature	Local investment

Plant Size

Total Facility	129,167	Square Feet
Production Floors	49,514	Square Feet
Warehouse Areas	8,611	Square Feet
Distribution Areas	3,229	Square Feet
Canteen & Dormitory Areas	27,986	Square Feet
Total Number of Buildings	3	
Total Number of Warehouses	2	
Total Number of Gates (Facility access points)	1	
Total Number of Gate Houses	1	

Use of Subcontractor

Name of Subcontractor	Service Type	Address
Nil	Nil	Nil
Other - Additional Subcontractors		
Other - Additional Subcontractors		

Shipment Methods to USA or other countries

By air	0.5	%
By sea	90	%
By truck	9.5	%
By rail	0	%
Other carrier type		

Total Employees

	On the date of the audit			
No. of Office Staffs	M	65	F	51
No. of Regular Staffs	M	57	F	95
No. of Contractual Staffs	M	0	F	0
No. of Temporary Staffs	M	0	F	0
Others	M	2	F	3
Total no. of employees	M	124	F	149

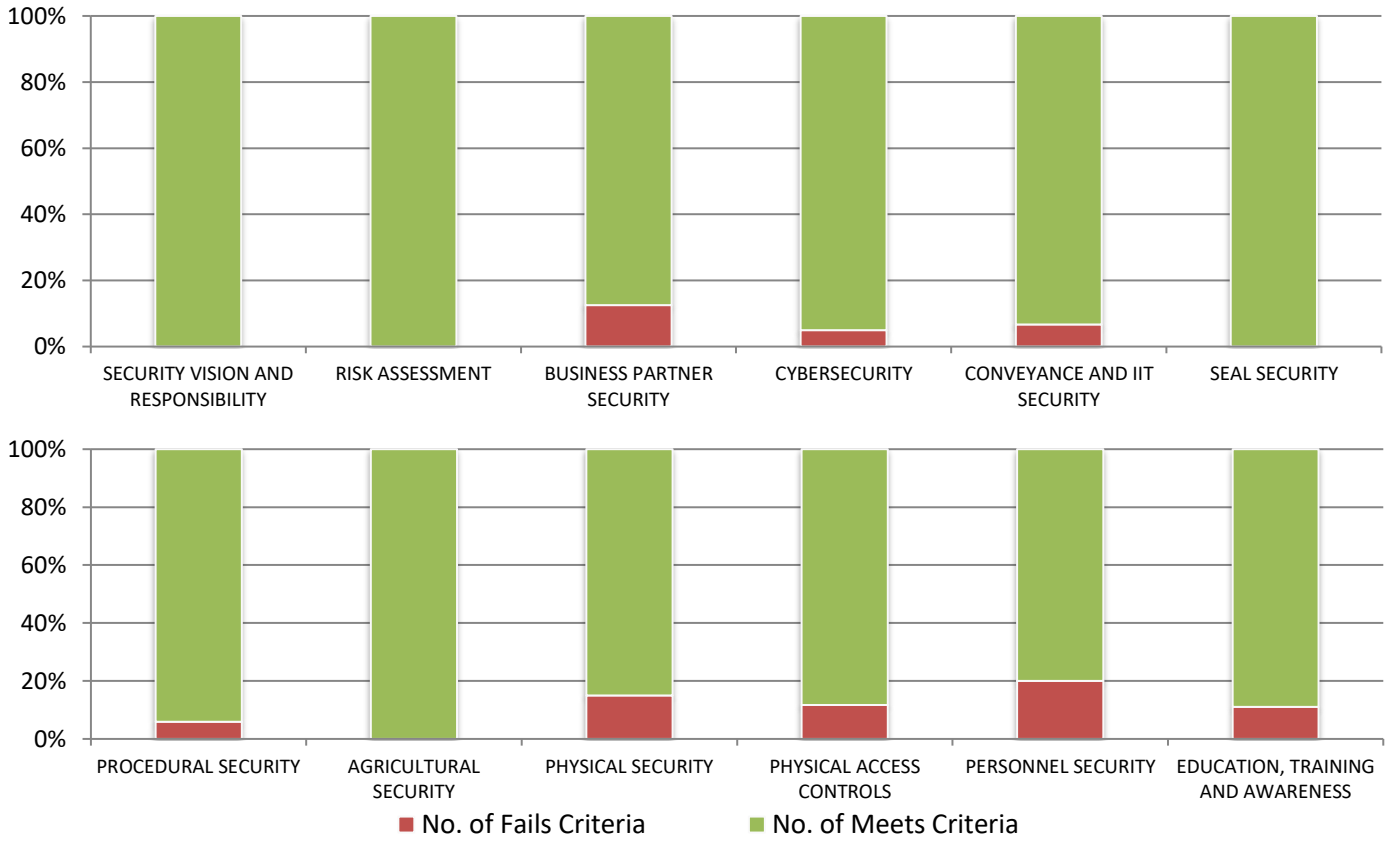
No. of Staff Recruited (last 12 months)	33	
No. of Staff Left (last 12 months)	15	
Average No. of Staff Total (last 12 months)	265	
Staff Turnover Rate (last 12 months)	6	%

Auditor Name:	Grace Xu
Technical Reviewer Name:	Jessica Ji

PERFORMANCE SUMMARY

		No. of Critical Violations	No. of Fails Criteria	No. of Meets Criteria	Section Score	Section Score (%)
1.0	SECURITY VISION AND RESPONSIBILITY	0	0	6	8	100%
2.0	RISK ASSESSMENT	0	0	7	10	100%
3.0	BUSINESS PARTNER SECURITY	0	1	7	12	92%
4.0	CYBERSECURITY	0	1	19	35	97%
5.0	CONVEYANCE AND IIT SECURITY	0	1	14	21	95%
6.0	SEAL SECURITY	0	0	7	14	100%
7.0	PROCEDURAL SECURITY	0	1	16	26	96%
8.0	AGRICULTURAL SECURITY	0	0	3	6	100%
9.0	PHYSICAL SECURITY	0	3	17	26	90%
10.0	PHYSICAL ACCESS CONTROLS	1	2	15	24	89%
11.0	PERSONNEL SECURITY	1	1	4	6	75%
12.0	EDUCATION, TRAINING AND AWARENESS	0	1	8	15	94%

CRITICAL VIOLATIONS	FINAL RESULT	OVERALL SCORE
2	Follow Up Audit or Desktop Review	94%



ACTIONS REQUIRED SUMMARY

Actions Required (Findings of MUST Criteria)	Section Number
It was suggested that the factory must check visitors' valid photo ID.	10.2.1
It was suggested that the factory must sign the C-PTAT Code of Conduct with workers.	11.5

ACTIONS RECOMMENDED SUMMARY

Actions Recommended (Findings of SHOULD Criteria)	Section Number
It was suggested that the factory should provide training to its business partners regarding C-TPAT's security requirements regularly.	3.2.4
It was suggested that the factory should established the policy to share cybersecurity threats with governments and business partners.	4.1.10
It was suggested that the factory should keep the GPS monitoring system records of their transportation for review.	5.7
It was suggested that the factory should separate international cargo from domestic cargo.	7.3
It was suggested that the factory should install alternate power sources.	9.14
It was suggested that the factory install and alarm for the camera.	9.15.4
It was suggested that the factory should keep the CCTV records of the factory boundary and entrance for at least 14 days.	9.15.5
It was suggested that the factory should check visitors' packages when they were arriving.	10.2.6
It was suggested that the factory provide training about warning indicators for money laundering and terrorist financing for workers.	12.1.6

SECTION 1.0 SECURITY VISION AND RESPONSIBILITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
1.1	Does the company have documented procedures for reviewing their supply chain security program?	Meets Criteria	MUST	The procedures are documented and adequately cover the company's supply chain security program.	
1.1.1	If yes, does this process include participation of different stakeholders within the company outside of security?	Meets Criteria	Should	The written policy includes participation of at least one employee outside of security or senior management, such as Human Resources, Information Technology, Import/Export Offices, Compliance, Logistics, etc.	
1.2	Is the company's point of contact (POC) on C-TPAT knowledgeable about the C-TPAT program requirements and security practices?	Meets Criteria	MUST	The company's C-TPAT point of contact has sufficient knowledge of the C-TPAT requirements and security practices.	
1.3	Does the company have a written policy on its commitment to supply chain security?	Meets Criteria	Should	The company does have a written policy on it's commitment to supply chain security.	
1.3.1	If yes, is the policy signed by a senior company official and reviewed annually?	Meets Criteria	Should	The written policy is signed by a senior company official (e.g. President, CEO, General Manager, Security Director, etc.) and reviewed annually.	
1.3.2	If yes, is that policy displayed in key locations?	Meets Criteria	Should	The written policy is displayed either on the company's website or in at least one physical location.	

Section 1.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	8
Total No. of Meets Criteria	6	Section Score (%)	100%

SECTION 2.0 RISK ASSESSMENT

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
2.1	For facilities within the company's control: Do they conduct a self-assessment of security practices, procedures and policies according to risk?	Meets Criteria	MUST	The company conducts security risk assessments of the areas under its control and a documented checklist or report is available.	
2.2	For facilities NOT within the company's control: Do they conduct a security-based risk assessments of their business partners and other facilities in their supply chain?	Meets Criteria	MUST	The company does conduct security risk assessments for facilities in their supply chain and the assessment has been clearly documented.	
2.2.1	If yes, does this assessment include consideration of relevant factors to supply chain security, such as volume, country of origin, routing, terrorist threat, etc.?	Meets Criteria	Should	The risk assessment includes all factors relevant to the supply chain security of the company.	
2.2.2	If yes, does the company maintain a list of all business partners by name, type of service provided, role in the supply chain, address of physical office location, contact information (e.g. telephone numbers, fax numbers, email), and contact name?	Meets Criteria	Should	The company does maintain a list of all business partners with all of the listed information.	
2.2.3	If yes, does this assessment include a mapping of the movement of cargo throughout the company's supply chain, including locations where cargo is "at rest" for an extended period of time?	Meets Criteria	Should	A cargo mapping was done and clearly indicates areas where cargo is "at rest" for an extended period of time.	
2.3	Is the security risk assessment reviewed or updated at least annually?	Meets Criteria	MUST	The security risk assessment has been reviewed or updated at least once within the past year.	
2.4	Does the company have procedures that address crisis management, business continuity, security recovery plans and business resumption?	Meets Criteria	Should	The company has procedures that address crisis management, business continuity, security recovery plans and business resumption.	

Section 2.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	10
Total No. of Meets Criteria	7	Section Score (%)	100%

SECTION 3.0 BUSINESS PARTNER SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
3.1	Does the company have a risk-based process for the **selection** of all business partners?	Meets Criteria	MUST	The company has a risk-based process for the selection of all business partners that includes financial soundness (e.g. credit check, bank reference, annual report), the capability of meeting contractual requirements and checks on activity related to money laundering and terrorism financing.	
3.1.1	If yes, do contracts with business partners address compliance with C-TPAT's minimum security criteria?	Meets Criteria	MUST	Written contracts specify that C-TPAT minimum security criteria are required to be met and maintained for all business partners (such as providing their C-TPAT SVI number or appropriate AEO registration).	
3.1.2	[Canada and Mexico] If yes, does the company only use C-TPAT certified highway carriers or ensure that the actual entity carrying the cargo across a U.S. land border meets C-TPAT's minimum security criteria?	Not Applicable	MUST	Not Applicable	The audit facility is not in Canada or Mexico.
3.2	Does the company have a risk-based process for the **monitoring** of all business partners?	Meets Criteria	MUST	The company has a risk-based process for monitoring business partners.	
3.2.1	If yes, does the company require business partners to complete a security questionnaire or provide evidence that their security practices meet C-TPAT's minimum security criteria?	Meets Criteria	MUST	The company's monitoring process includes sufficient checks of their business partner's security practices with respect to C-TPAT's requirements.	
3.2.2	If yes, does this include timely correction of deficiencies in their business partners' security practices?	Meets Criteria	MUST	Identification and correction of deficiencies was documented in a checklist or a report.	
3.2.3	If yes, is the security assessment of the company's business partners updated on a regular basis?	Meets Criteria	Should	The security assessment of the company's business partners is regularly updated as dictated by circumstances or risk.	
3.2.4	If yes, does the company provide guidance or training to its business partners regarding C-TPAT's security requirements?	Fails Criteria	Should	No C-TPAT security training has been provided to its business partners.	The factory did not provide training to its business partners regarding C-TPAT's security requirements.
3.3	Does the company have a social compliance program that prohibits the use of forced, imprisoned, indentured, or indentured child labor in the production of its products?	Meets Criteria	Should	The company has a sufficient social compliance program.	

Section 3.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	1
Total No. of Fails Criteria	1	Section Score	12
Total No. of Meets Criteria	7	Section Score (%)	92%

SECTION 4.0 CYBERSECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
4.1	Does the company have comprehensive written policies or procedures covering IT protection and cybersecurity?	Meets Criteria	MUST	The company has at least one written policy or procedure to protect its IT systems.	
4.1.1	If yes, are the policies and procedures reviewed, updated and endorsed by management at least once a year?	Meets Criteria	MUST	The policies and procedures have been reviewed at least once within the past year.	
4.1.2	If yes, do the procedures clearly state what is considered abuse of its IT systems?	Meets Criteria	MUST	Abuse of its IT systems is clearly defined and communicated to all employees.	
4.1.3	If yes, does the company have a clear process for disciplining violators of these procedures?	Meets Criteria	MUST	The process for disciplining violators of its cybersecurity policies is both clear and enforced.	
4.1.4	If yes, does the company have processes to identify, prevent and address the loss of data in the event of attacks via social engineering (such as phishing)?	Meets Criteria	MUST	The company has a clear process for helping employees identify when they are the target of a social engineering attack and what to do to prevent the loss of data.	
4.1.5	If yes, does the company only allow remote access to its IT systems through secure technologies, such as virtual private networks (VPNs)?	Meets Criteria	MUST	Either remote access is prohibited or only allowed via secure technologies, such as VPNs.	
4.1.6	If yes, do all employee personal devices used for company business adhere to the company's cybersecurity policies and procedures?	Meets Criteria	MUST	Either employees are not allowed to conduct company business on personal devices or all such devices are compliant with the company's cybersecurity polices and procedures.	
4.1.7	If yes, does the company utilize an effective employee ID system to control access only to IT systems necessary for the performance of their duties?	Meets Criteria	MUST	IT systems are adequately restricted to only employees who need access to perform their duties.	
4.1.8	If yes, are employees assigned individual accounts that require a periodic change of password?	Meets Criteria	MUST	All employees are assigned individual accounts that require a password change at least once every 90 days.	
4.1.9	If yes, does the company's IT systems include automatic time-outs of users and the disabling of accounts after a number of failed log-in attempts?	Meets Criteria	Should	The company's IT system automatically times-out users and disables their accounts after several failed log-in attempts.	
4.1.10	If yes, does the company have a policy to share cybersecurity threats with governments and business partners?	Fails Criteria	Should	The company does not share cybersecurity threats externally.	The factory did not established the policy to share cybersecurity threats with governments and business partners.
4.2	Does the company use software to conduct business or manage data?	Meets Criteria	MUST	The company has at least one piece of software used to conduct business or manage data.	
4.2.1	If yes, is the software capable of identifying and preventing unauthorized access?	Meets Criteria	MUST	The company's software has sufficient safeguards against unauthorized access of IT systems.	
4.2.2	If yes, does the company have sufficient software solutions to protect their IT systems from malware (viruses, spyware, worms, Trojans, etc.) and external intrusions?	Meets Criteria	MUST	The company employs software to counter malware and prevent external intrusion of its IT systems.	
4.2.3	If yes, does the company's software receive automatic security updates?	Meets Criteria	MUST	The company's software does receive automatic security updates and is currently up-to-date.	
4.2.4	If yes, does the company prevent the use of counterfeit or improperly licensed technology or software?	Meets Criteria	Should	All software and technology is properly licensed.	
4.2.5	If yes, are all sensitive and confidential data stored in an encrypted format and backed up at least once a week?	Meets Criteria	Should	All sensitive and confidential data is encrypted and backed up at least once a week.	
4.3	Does the company conduct business using hardware or store data on physical electronic media?	Meets Criteria	MUST	The company has at least one piece of hardware or physical media used to conduct business or store data.	
4.3.1	If yes, does the company regularly test the security of their IT infrastructure and, if vulnerabilities are found, implement corrective actions promptly?	Meets Criteria	MUST	IT security has been tested within the past year and any corrective actions have been or are in the process of being implemented.	
4.3.2	If yes, does the company ensure regular inventories are done for all media, hardware and/or other IT equipment and follow appropriate industry guidelines for media sanitization upon disposal?	Meets Criteria	MUST	The company has an accurate inventory of its media and IT equipment and has clear processes for appropriate disposal when no longer needed.	

Section 4.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	1	Section Score	35
Total No. of Meets Criteria	19	Section Score (%)	97%

SECTION 5.0 CONVEYANCE AND INSTRUMENTS OF INTERNATIONAL TRAFFIC (IIT) SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
5.1	Does the company have written procedures covering both security and agricultural inspections of containers, cargo handling and storage areas?	Meets Criteria	MUST	The companies procedures include the processes for conducting security and agricultural inspections of containers, cargo handling and storage areas.	
5.1.1	If yes, does this include appropriate seven- or eight-point inspections of all empty containers, unit load devices (ULDs), and other IIT, both refrigerated and unrefrigerated?	Meets Criteria	MUST	An appropriate seven- or eight-point inspection is conducted on all empty containers, ULDs and other IIT.	
5.1.2	If yes, does this include inspection of all external hardware to ensure that it can withstand attempts to remove it and detect any tampering?	Meets Criteria	MUST	All external hardware (e.g. doors, handles, rods, hasps, rivets, brackets, and all other parts of the locking mechanism) of containers or other IIT are inspected and in working order.	
5.1.3	If yes, are there procedures for the cleaning of containers or areas found to have pest contamination?	Meets Criteria	MUST	There are adequate procedures for the cleaning of pest contaminated containers or areas and the records of any decontaminations are kept for at least one year.	
5.1.4	If yes, are all the points of the inspection documented on a checklist and included in the shipping documentation sent to the recipient?	Meets Criteria	Should	Inspections are adequately documented on a checklist and sent to the recipient.	
5.1.5	If yes, are these inspections done in a secured area and, if available, monitored via CCTV?	Meets Criteria	Should	All inspections occur in secured and monitored areas.	
5.2	Is the integrity of containers and other IIT maintained during loading/stuffing/packing using clearly written procedures?	Meets Criteria	Should	Written procedures exist covering loading/stuffing/packing that ensure the integrity of containers or other IIT.	
5.3	Are random searches conducted by management on containers and other IIT post-inspection?	Meets Criteria	Should	At least one random search has been conducted in the past year.	
5.4	Does the company have secure areas where they handle their cargo?	Meets Criteria	MUST	All of the handling of cargo occurs in secure areas.	
5.4.1	If yes, does this include a secure storage area for empty and full containers and other IIT to prevent unauthorized access?	Meets Criteria	MUST	Containers and other IIT are only stored in secure areas (e.g. an area with a locked perimeter fence and adequate lighting).	
5.4.2	If yes, are loading docks for trucks and pick-ups/deliveries separate from all other vehicles and traffic?	Meets Criteria	Should	Truck and pickup/delivery traffic are adequately separated from all other vehicles and traffic.	
5.4.3	If yes, is there a secured area for truck and pick-up/delivery drivers to wait while cargo is loaded and unloaded?	Meets Criteria	Should	There is a secured waiting area for drivers and they are required to wait in this area during loading and unloading operations.	
5.5	Does the company have written procedures for reporting incidents, such as thefts, tampering and unmanifested items, to affected business partners and law enforcement agencies?	Meets Criteria	MUST	The company does report incidents of thefts, tampering or unmanifested items to relevant business partners in its supply chain and any law enforcement agencies as required.	
5.6	Are there procedures to track the movement of all cargo during transit via their transportation providers?	Meets Criteria	Should	Procedures and security controls exist to track the movement of all cargo during transit. These procedures include reconciling the goods against the manifest and ensuring they are accurately marked.	
5.7	Does the company have access to their transportation providers GPS monitoring system so that they can track their shipments?	Fails Criteria	Should	Either there is no GPS monitoring system or the company does not have access to it.	Based on document review, the factory did not provide the GPS monitoring system records of their transportation.
5.8	[Canada and Mexico] Does the company have a "no-stop" policy with regards to unscheduled stops for shipments if they are in proximity to a U.S. land border?	Not Applicable	Should	Not Applicable	The audit facility is not in Canada or Mexico.
5.9	[Canada and Mexico] Does the company conduct final inspections verifying seal and container integrity before crossing a U.S. border in high risk areas?	Not Applicable	Should	Not Applicable	The audit facility is not in Canada or Mexico.

Section 5.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	2
Total No. of Fails Criteria	1	Section Score	21
Total No. of Meets Criteria	14	Section Score (%)	95%

SECTION 6.0 SEAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
6.1	Does the company have written procedures to control, record and affix ISO 17712 compliant seals on all containers and IIT?	Meets Criteria	MUST	The company has sufficient written procedures on security seals.	
6.1.1	If yes, are these procedures maintained and accessible at the local, operating level?	Meets Criteria	MUST	The procedures are accessible at the local level.	
6.1.2	If yes, are these procedures reviewed and updated at least once a year?	Meets Criteria	MUST	The procedures have been updated within the past year.	
6.1.3	If yes, do they document that all seals meet or exceed the current ISO 17712 standard?	Meets Criteria	MUST	All seals meet or exceed the current ISO 17712 standard.	
6.1.4	If yes, are all containers and IIT secured with a ISO 17712 compliant seal immediately after loading/stuffing/packing?	Meets Criteria	MUST	All containers and IIT are immediately sealed after loading/stuffing/packing.	
6.1.5	If yes, are all seals verified using the VVTT process?	Meets Criteria	MUST	All seals are verified using the VVTT process.	
6.2	Are periodic audits of seals conducted that include an inventory of stored seals, reconciliation against seal documentation, and the periodic verification of seal numbers on containers or IIT?	Meets Criteria	MUST	At least one audit of security seal inventory and procedures has been conducted in the past year.	

Section 6.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	14
Total No. of Meets Criteria	7	Section Score (%)	100%

SECTION 7.0 PROCEDURAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
7.1	If cargo is held at the facility for an extended period of time, such as overnight, is it stored in a secure area?	Meets Criteria	MUST	All cargo stored overnight or for extended periods of time is secured from unauthorized access.	
7.2	Does the company ensure that cargo staging and storage areas are regularly inspected for pest contamination?	Meets Criteria	MUST	The cargo staging and storage areas have been inspected for pest contamination within the last year.	
7.3	Does the company keep international cargo separate from domestic cargo?	Fails Criteria	Should	International and domestic cargo are not adequately segregated.	Based on onsite observation, the factory did not separate international cargo from domestic cargo.
7.4	Does the company keep hazardous or dangerous cargo separate from other cargo?	Not Applicable	Should	Not Applicable	The audited facility had no hazardous or dangerous cargos. Only hats were manufactured in the factory.
7.5	Does the facility have a designated employee, preferably a security officer, to supervise the loading/stuffing/packing of cargo into containers and IIT?	Meets Criteria	Should	There is a designated employee responsible for supervising the loading/stuffing/packing of cargo.	
7.6	Does the company require digital images to be taken of the properly installed seals during loading/stuffing/packing to be compared with the images taken at the destination?	Meets Criteria	Should	Digital images of seals are taken and compared to the images at the destination.	
7.7	Are all cargo properly marked, counted, weighed, documented and reported on the manifests and bills of lading (BOL)?	Meets Criteria	MUST	Cargo are properly marked, counted, weighed, documented, and reported on the manifests and bills of lading (BOL).	
7.8	Is all information used in the clearing of cargo legible, complete, accurate, protected against exchange, loss, or the introduction of erroneous information and reported on time?	Meets Criteria	MUST	All of the information used in the clearing of cargo meets these requirements.	
7.9	Does the company have procedures to verify both arriving and departing cargo against manifests, purchase orders, or other shipment documentation?	Meets Criteria	MUST	There are procedures to protect and verify shipments. They include verifying all cargo against the manifests, purchase orders or other shipment documentation.	
7.9.1	If yes, do these procedures cover the process for resolving any cargo discrepancies (shortages, overages, etc.) found?	Meets Criteria	MUST	The company has written procedures in place to resolve all cargo discrepancies prior to cargo being released or received. Those procedures include having a security guard or shipping supervisor conduct an investigation where appropriate.	
7.10	Are seal numbers electronically printed on the BOL or other shipping documents and transmitted to the receiver of the delivery prior to departure?	Meets Criteria	Should	Seal numbers are recorded on shipping documents and sent to the recipient of the delivery.	
7.11	If paper documents are used for recording cargo or shipment information, are these documents properly secured?	Meets Criteria	Should	Either no paper documents are used or they are properly secured, such as in a safe or locked filing cabinet, to prevent unauthorized access.	
7.12	Does the company have written procedures for challenging unauthorized or unidentified persons attempting to gain access to the facility?	Meets Criteria	MUST	The written procedures clearly state how employees can identify, challenge and address unauthorized or unidentified persons trying to access the facility.	
7.13	Are all cargo and shipping documentation reviewed by personnel appropriately training on how to identify suspicious cargo shipments?	Meets Criteria	MUST	There is evidence of regular reviews of documents for suspicious activity within the past year by appropriately trained personnel.	
7.14	Does the company have procedures for a prompt internal investigation of any security-related incident, which is made available to CBP or other law enforcement agencies upon request?	Meets Criteria	MUST	There is a procedure for internal investigations, which allows for the results of any investigations to be disclosed to CBP or other law enforcement agencies.	
7.15	Does the company have written procedures for reporting security incidents to relevant customs or law enforcement agencies, depending on the severity of incident?	Meets Criteria	MUST	The procedures cover the reporting of security incidents, including the process for escalating the issue internally and to relevant external agencies.	
7.15.1	If yes, does the company have documented procedures for anonymously reporting security incidents to relevant parties?	Meets Criteria	Should	Security incidents can be reported anonymously.	
7.15.2	If yes, is there an incentive scheme which encourages staff to report security incidents?	Meets Criteria	Should	There is an incentive scheme for reporting security incidents.	

Section 7.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	1
Total No. of Fails Criteria	1	Section Score	26
Total No. of Meets Criteria	16	Section Score (%)	96%

SECTION 8.0 AGRICULTURAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
8.1	Does the company have written procedures to prevent pest contamination from wood packaging materials (WPM) (see the IPPC's International Standards for Phytosanitary Measures No. 15)?	Meets Criteria	MUST	The company has written procedures covering pest contamination from wood packaging materials.	
8.1.1	If yes, do all wood packaging aterials (WPM) used at the facility bear a mark (conforming to Annex 2 of ISPM 15) indicating that the WPM has been subjected to approved phytosanitary treatment?	Not Applicable	MUST	Not Applicable	The audited facility had no wood packaging materials for all cargos.
8.1.2	If yes, do these procedures instruct personnel how to manage reused, repaired or remanufactured WPM so that they meet all treatment and marking standards (according to ISPM 15)?	Meets Criteria	MUST	The procedures clearly indicate how personnel can re-treat and re-mark any reused, repaired or remanufactured WPM.	
8.1.3	If yes, do these procedures instruct personnel how to manage and securely dispose of pest contaminated or otherwise non-compliant WPM according to the requirements of ISPM 15 and/or the country's National Plant Protection Organization (NPPO)?	Meets Criteria	MUST	The procedures note an appropriate process for disposal of pest contaminated or non-compliant WPM.	

Section 8.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	1
Total No. of Fails Criteria	0	Section Score	6
Total No. of Meets Criteria	3	Section Score (%)	100%

SECTION 9.0 PHYSICAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
9.1	Are facilities designed and constructed with materials appropriate to prevent unauthorized access?	Meets Criteria	MUST	Buildings are designed and constructed with materials appropriate to prevent unlawful entry (e.g., brick, stone, concrete, heavy gauge steel)	
9.2	Does the facility have perimeter fencing or walls on all sides of a height of 6 ft (1.8 m) and, where appropriate, interior fencing or walls to segregate cargo such as domestic, international, high value, and/or hazardous materials?	Meets Criteria	Should	The facility has perimeter fencing or walls on all sides of a height of 6 ft. (1.8 m) and adequate interior barriers to segregate cargo.	
9.3	Does the facility have functional locking devices for all internal and external doors, windows, gates and fences, where appropriate to prevent unauthorized access?	Meets Criteria	MUST	All appropriate locations have functional locking devices and are protected against tampering or intrustion (e.g. windows are protected by wire mesh, protective coatings, or are made of heavy gauge Plexiglas).	
9.4	Does the facility have written procedures to control the issuance of keys, and are keys recovered and/or locks changed when employees who have them change positions within or leave the company?	Meets Criteria	Should	The facility has logs of keys and has a documented procedure for lost keys including changing locks when relevant employees change positions within or leave the company.	
9.5	Does the facility have internal and external lighting in all required areas (e.g. entrances and exits, cargo handling and storage areas, the factory perimeter, parking areas, etc.)?	Meets Criteria	MUST	The facility has adequate internal and external lighting in all key areas that is properly maintained and functional.	
9.6	Does the facility monitor all external access points either using manned positions or technology?	Meets Criteria	MUST	All external access points are monitored either via manned positions or remotely using technology.	
9.7	Is parking at the facility authorized using a decal system or using passes issued from a security gate?	Meets Criteria	Should	All parking is authorized via passes from a security gate or through a vehicle decal system.	
9.8	Is parking for private vehicles (employees, visitors, vendors, contractors, etc.) clearly separated from cargo staging areas and loading docks?	Meets Criteria	Should	Parking for private vehicles is restricted to designated areas separate from cargo staging and loading docks.	
9.9	Does the facility have documented policies for the use, maintenance and protection of security technology (e.g. building, fencing, gates, lights, alarm system and CCTV) including regular inspections?	Meets Criteria	MUST	Procedures exist for the use, maintenance and protection of security technology including inspections at least once a year.	
9.10	Is access to all security technology infrastructure physically restricted?	Meets Criteria	MUST	All security technology is physically secured from unauthorized access.	
9.11	Are security technologies used to prevent unauthorized access to sensitive areas?	Meets Criteria	Should	All sensitive areas are adequately protected from unauthorized access using technologies such as alarms, access control devices, or camera systems.	
9.12	Does the facility have a security alarm system, which is appropriately managed when employees leave the company?	Meets Criteria	Should	The facility has logs of alarm codes issued, and has a procedure for resetting alarm codes when employees change positions within or leave the company. The alarm is in proper working order.	
9.13	Does the company only use licensed or certified resources when designing or installing security technology?	Meets Criteria	Should	All security technology is from licensed or certified sources.	
9.14	In event of power loss, are all critical security technology systems connected to alternate power sources?	Fails Criteria	Should	There is no alternative power source for critical security technology systems.	The factory did not install alternate power sources for the critical security technology systems.
9.15	Are cameras systems (e.g. CCTV) used?	Meets Criteria	Should	The facility uses camera systems.	
9.15.1	If yes, are these camera systems used to monitor the facility's premises including the key areas related to cargo and container security?	Meets Criteria	MUST	Entrances to the property or parking areas and other critical areas are monitored by CCTV.	
9.15.2	If yes, are these camera systems set to record on a 24 hour, 7 days a week basis and at the highest picture quality setting reasonably available?	Meets Criteria	MUST	The cameras record on a 24 hour, 7 days a week basis and the picture quality is sufficient.	
9.15.3	If yes, are periodic reviews of the camera footage conducted by relevant personnel and documented in writing including any corrective actions that were taken?	Meets Criteria	MUST	At least one review of camera footage has been conducted and documented in the past year.	
9.15.4	If yes, do these camera systems have an alarm or other notification feature that signals when the camera is not operating properly or not recording?	Fails Criteria	Should	The cameras do not have an alarm or notification feature.	There was no alarm or other notification feature that signals when the camera is not operating properly or not recording.
9.15.5	If yes, is camera footage of all key import and export processes maintained for a sufficient amount of time to allow for investigations of monitored shipments?	Fails Criteria	Should	Camera footage is not maintained or is maintained for less than 14 days.	The CCTV records of the factory boundary and entrance was only kept for 10 days.

Section 9.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	3	Section Score	26
Total No. of Meets Criteria	17	Section Score (%)	90%

SECTION 10.0 PHYSICAL ACCESS CONTROLS

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
10.1	Does the company have a documented procedure defining access controls for employees and drivers?	Meets Criteria	MUST	The company has a documented procedure defining access controls.	
10.1.1	If yes, are all employees required to present identification upon entering the facility?	Meets Criteria	MUST	Identification is required for all employees and checked upon entrance.	
10.1.2	If yes, are drivers required to present photo identification prior to cargo being received or released to/from their custody?	Meets Criteria	MUST	Drivers are required to present photo identification prior to cargo being received or released to/from their custody.	
10.1.3	If yes, does the company maintain a cargo pickup log for all registered drivers?	Meets Criteria	MUST	All drivers maintain a cargo pickup log.	
10.1.4	If yes, are deliveries and pickups allowed by appointment only?	Meets Criteria	Should	Deliveries or pickups are only allowed by appointment.	
10.1.5	If yes, do carriers notify the company before drivers arrive at the facility with relevant details of the pickup?	Meets Criteria	Should	Carriers notify the company of all of its pickups with the estimated time of arrival for the scheduled pick ups, the name of the driver, and the truck number.	
10.1.6	If yes, is pickup and delivery of cargo limited only to monitored areas of the facility?	Meets Criteria	Should	Pickup or delivery of cargo only occurs inside of monitored areas.	
10.1.7	If yes, are arriving packages and mail periodically screened for dangerous materials or contraband before being admitted?	Meets Criteria	Should	Packages and mail are periodically screened for dangerous materials or contraband prior to dissemination.	
10.2	Does the company have a documented procedure defining access controls for visitors?	Meets Criteria	MUST	There are documented procedures defining visitor access to the facility.	
10.2.1	If yes, are all visitors required to present a valid photo ID for positive identification before being allowed access to the facility?	Fails Criteria	MUST	There are no photo identification requirements for visitors to enter the facility or the requirement is inadequately enforced.	Based on onsite observation, the factory did not require visitors to present a valid photo ID.
10.2.2	If yes, are all visitors issued temporary ID's?	Meets Criteria	MUST	Temporary ID's are issued for all visitors and they are required to wear or present them while inside the facility.	
10.2.3	If yes, does the company maintain a log of all visitors entering the facility?	Meets Criteria	MUST	All visitors' names and companies are written in a logbook at either the security gate, loading area or the front office.	
10.2.4	If yes, are employee escorts required for all visitors while on the premises?	Meets Criteria	MUST	Employee escorts are required to remain with visitors throughout their visit.	
10.2.5	If yes, are visitors required to have an appointment prior to being granted admission to the facility?	Meets Criteria	Should	All visitors are required to have an appointment prior to being granted admission to the facility.	
10.2.6	If yes, are all visitor's packages screened prior to being granted admission to the facility?	Fails Criteria	Should	There is no procedure or the procedure is inadequate to screen visitor's packages prior to being granted admission to the facility.	When visitors entered the factory, the factory did not check their packages.
10.3	Does the facility employ security guards?	Meets Criteria	Should	Security guards are employed.	
10.3.1	If yes, are there written work instructions for the security guards that management periodically checks for compliance and appropriateness?	Meets Criteria	MUST	There are adequate work instructions for security guards that include performing scheduled security patrols during working hours.	

Section 10.0 Summary

Total No. of Critical Violations	1	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	2	Section Score	24
Total No. of Meets Criteria	15	Section Score (%)	89%

SECTION 11.0 PERSONNEL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
11.1	Does the company verify the information on employment applications submitted from prospective employees prior to employment as permitted by law?	Meets Criteria	MUST	Management verifies information on applications as permitted by law. Verification results are maintained for the length of employment.	
11.2	Does the company interview prospective employees as permitted by law?	Meets Criteria	MUST	Prospective employees are interviewed as permitted by law. All records are kept in a secure place for the length of their employment and may be submitted to the appropriate authority upon request.	
11.3	Does the company perform background checks of prospective employees prior to employment as permitted by laws?	Meets Criteria	Should	Background checks are performed on all prospective employees as permitted by law.	
11.4	Does the company conduct periodic background checks or screening on existing employees as permitted by law?	Meets Criteria	Should	Periodic rescreening of employee background checks are performed on existing employees as permitted by law.	
11.5	Are employees required to sign a Code of Conduct?	Fails Criteria	MUST	No Code of Conduct exists or some employees are not required to sign it.	Workers did not sign C-PTAT Code of Conduct.

Section 11.0 Summary

Total No. of Critical Violations	1	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	1	Section Score	6
Total No. of Meets Criteria	4	Section Score (%)	75%

SECTION 12.0 EDUCATION, TRAINING AND AWARENESS

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
12.1	Does the company provide security and agricultural training to new employees that is appropriate to their position and job responsibilities?	Meets Criteria	MUST	Comprehensive training is provided to all new employees that covers the company's security and agricultural policies and procedures. Completion is documented using training logs or electronics records.	
12.1.1	If yes, are employees provided training to on how to conduct security and agricultural inspections of containers and other IIT?	Meets Criteria	MUST	All relevant employees are trained on how to properly conduct security or agricultural inspections that includes topics such as signs of hidden compartments, contraband concealed in naturally occurring compartments and signs of pest contamination.	
12.1.2	If yes, are employees provided training on the company's cybersecurity policies and procedures?	Meets Criteria	MUST	Employees are trained on the company's cybersecurity policies and procedures, including clear definition of their roles and responsibilities for securing IT systems.	
12.1.3	If yes, are employees managing security technology systems provided training on or have previous experience in their operation and maintenance?	Meets Criteria	MUST	Personnel have been trained or have previous experience in operating security technology.	
12.1.4	If yes, are employees trained on how to recognize suspicious situations and the methods to report them?	Meets Criteria	MUST	The training provided includes details on identifying and reporting suspicious activity, such as how and what to report, to whom it should be reported and what to do after reporting.	
12.1.5	If yes, are employees trained on how to identify and prevent the spread of pest contamination?	Meets Criteria	MUST	Personnel involved in the handling or storage of cargo have had at least one training on the identification and prevention of pest contamination.	
12.1.6	If yes, are employees trained or provided regular updates on warning indicators of trade-based money laundering and terrorism financing?	Fails Criteria	Should	No or inadequate threat awareness training is provided to employees.	Based on document review, the factory did not provide training about warning indicators for money laundering and terrorist financing.
12.1.7	If yes, do these trainings include measures to verify that the training objectives have been met, such as quizzes, exercises or audits?	Meets Criteria	Should	Training objectives are verified using quizzes, exercises or audits to confirm that employees acknowledge and understand the policies and procedures.	
12.2	Are refresher trainings conducted, either on a regular basis or after incidents, to ensure that employees are current on all updated policies and procedures?	Meets Criteria	MUST	At least one refresher training or update has been provided to existing employees within the last year.	

Section 12.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	1	Section Score	15
Total No. of Meets Criteria	8	Section Score (%)	94%

END OF CHECKLIST

PHOTO REPORT

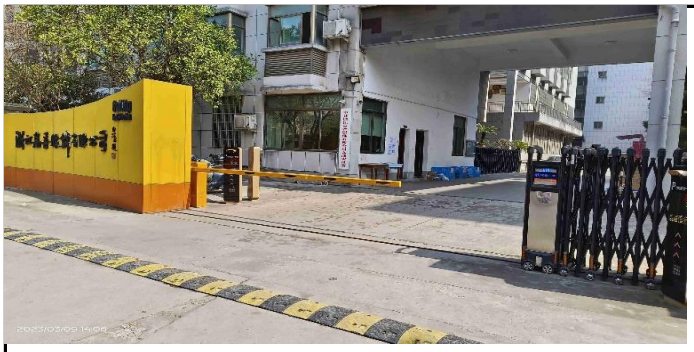


Photo Remarks: Facility Entrance

Photo Remarks: Facility name

Photo Remarks: Facility Building

Photo Remarks: Security warnings

Photo Remarks: Loading & Docking Area

Photo Remarks: Security guards

Photo Remarks: Packing Area

Photo Remarks: Visitors' cards

Photo Remarks: Employee's card

Photo Remarks: Fence

Photo Remarks: The camera and light

Photo Remarks: CCTV records

Photo Remarks: The empty cargo inspection tools

Photo Remarks: The seals storage area.

Photo Remarks: Finished goods warehouse

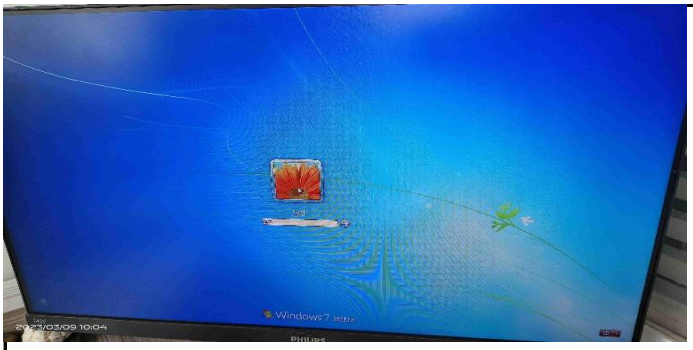


Photo Remarks: The password was set.

Photo Remarks: The driver resting room

Photo Remarks: Locked window in all workshops and warehouses

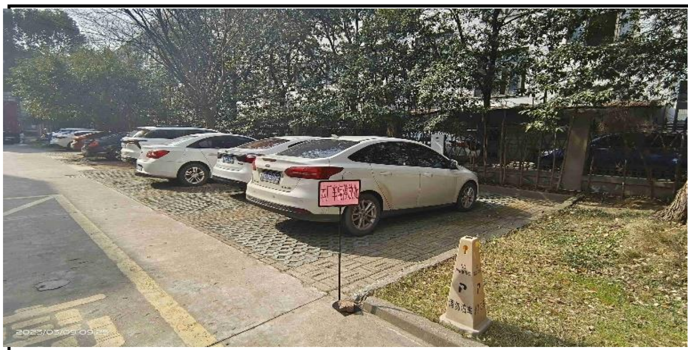


Photo Remarks: The private car parking area

浙江高普服饰有限公司
访客、车辆进出登记表

日期	姓名	单位	身份证号码/驾驶证号码	车牌号码	入厂事由	被访人	入厂时间	出厂时间	访客证编号	访客证回收	值班员	备注

Photo Remarks: Visitor in/out records

浙江高普服饰有限公司
集装箱车辆出入登记表

日期	司机姓名	驾驶证号/身份证号	是否核实	车牌号码	集装箱号	封条号	提单号	出入时间 入时间	出入时间 出时间	访客证号	检查状况 证件收回	值班保

Photo Remarks: Cargo in/out records

Photo Remarks: 9.15.5 The CCTV records of the factory boundary and entrance was only kept for 10 days.