



Factory Security Assessment - General Merchandise and Food - Country Rated Medium Risk for Supply Chain Security -

Factory Profile

Wal-Mart Factory ID #	36208191		
Factory Name	Suzhou Fuyougang Can Products Co., Ltd		
Factory Street Address	No.28-9, Shuangma Road, Dianshanhu Town, Kunshan City, Suzhou City, Jiangsu Province, China		
	Nil		
Factory City and Country	Suzhou	China	
Wal-Mart SCS Audit Request ID #	10279330		
Factory Responsible Person Name	Ms. Zhou Guangmei/ HR		
Contact Number	86-0512-57488409		
Date of Security Audit	Sep-27-2018		

OVERALL SCORE	82		
RISK RATING	Medium Risk Priority		

Audit Company

Audit Company Name	Bureau Veritas
Audit Team	BVCN074 .

Audit Overview

Audit attendance	Ms. Zhou Guangmei/ HR
Present at the opening meeting?	Yes
Present at the closing meeting?	Yes

Company Profile

Company name	Suzhou Fuyougang Can Products Co., Ltd		
Contact name	Ms. Zhou Guangmei/ HR		
Address 1	No.28-9, Shuangma Road, Dianshanhu Town, Kunshan City, Suzhou City, Jiangsu Province, China		
Address 2	Nil		
City	Suzhou		
State	Jiangsu		
Country	China	Postal Code	215345
Phone	86-0512-57488409		
Fax	86-0512-57488410		
Email	FYG2015@aliyun.com		
Website	www.fyg-sz.com		
Number of employees			
Permanent	71		



BUREAU
VERITAS

Temporary	0
Overseas / Migrant	0
Total	71

Business Overview

Industry	Hardlines		
Key / Main product	Can		
Country of operation	China		
	Yes	No	Not Applicable
Participation in security initiatives	●		
Description of security initiative	ISO-A, -		

Facility Structure

Number of buildings	
Distribution	1
Production	1
Warehouse	1
Container yards	1
Other	1
Total	5
Facility size	4000M. Sq.
Facility size outside grounds	1000M. Sq.
Warehouse customs bonded	NO
Free trade zone	NO
Logistics/Transportation for shipments to US	
Trucks owned By Company	No
Percent of goods exported to US	
By air	0
By sea	100
By rail	0
By truck	0
Description of "other" buildings	One 2-storey office building

Overall Comment

Percent of goods exported to US: 40%



SECURITY AREA TO IMPROVE

Findings and issues identified within below sections are essential to attain the Walmart Supply Chain Security requirements. The supplier/facility is recommended to take the necessary Corrective Action Plans for below findings to improve the overall security performance.

Section: Personnel Security

- **Finding:** Some personnel file is not maintained for each employee.
It was noted that though personnel files were maintained for each employee, no information such as 'Working experience', 'Family background' and 'Education background' etc. was shown on their personnel files.
Recommendation: Personnel file must be maintained for each employee.
- **Finding:** The written Employee Termination policy does not include removing the identification badge or facility access or system access for an employee who is terminated or resigns.
It was noted that although the factory has a written Employee Termination policy to remove the identification badge, facility access and system access for an employee who is terminated or resigned. However, the policy was not applied to the employees who applied for long term leave. (E.g. for the female employee who had applied for 128 days maternity leave).
Recommendation: The facility must have written Employee Termination policy to remove the identification badge, facility access, and system access for an employee who is terminated or resigns.

Section: Threat Awareness

- **Finding:** The facility does not provide Threat Awareness Training during new hire orientation and/or then every 12 months as refresher training to all employees.
It was noted that although facility provided Threat Awareness Training to new hire orientation and refresher training to all employees. Interviewed employees did not know the Threat Awareness Program.
Recommendation: The facility must provide Threat Awareness Training during new hire orientation and then every 12 months as refresher training to all employees.
- **Finding:** Employees who report suspicious activity and security violations are not given some form of encouragement.
It was noted that the no document evidence was available to show that employees who reported suspicious activity and security violations were given some form of encouragement while such policy had been established.
Recommendation: Employees who report suspicious activity and security violations must be given some form of encouragement.

Section: Physical Access Controls

- **Finding:** The facility management do not review and update employee lists that authorize access to sensitive and restricted work areas.
The factory had a written policy to require that only authorized employees are permitted access to sensitive or restricted areas. However, the factory didn't review and update employee lists that authorize access to sensitive and restricted work areas.
Recommendation: The facility management must review and update employee lists that authorize access to sensitive and restricted work areas.
- **Finding:** The facility does not have written policy to ensure that only authorized employees are permitted access to sensitive or restricted areas.
During this audit, when the auditor and factory accompanying person entered the packing workshop, there was nobody came to check the auditor and accompanying person's identification.
Recommendation: The facility must have written policy to ensure that only authorized employees are permitted access to sensitive or restricted areas.
- **Finding:** The facility does not have written and implemented procedure that requires a visitor and a pick-up/delivery driver to show photo identification before entry is permitted.
It was noted that auditor was not required to show photo identification when entered the factory while such policy was established and such training had been provided to the security guards.
Recommendation: The facility must have written and implemented procedure that requires a visitor and a pick-up/delivery driver to show photo identification before entry is permitted.



Section: Physical Security

- **Finding:** Access to outside lighting switches or controls is not restricted to only authorized employees or the security guard supervisor.
It was noted that the access to lighting switches or controls were not restricted to only authorized employees or the security guard supervisor.
Recommendation: Access to outside lighting switches or controls must be restricted to only authorized employees or the security guard supervisor.
- **Finding:** During darkness, some of the facility perimeter fence/wall is not well illuminated.
It was noted that most sensitive areas were installed with sufficient lighting equipment. However, per factory tour, it was noted that no lighting equipment was installed along the fencing wall.
Recommendation: During darkness, the facility perimeter fence/wall must be well illuminated.

Section: Container/Trailer Security

- **Finding:** Recording of CCTV used to capture container/trailer loading is not kept for a minimum of 30 days.
The CCTV recordings of loading/unloading area were only kept for 1 day instead of kept for at least 30 days.
Recommendation: Recording of CCTV used to capture container/trailer loading must be kept.

Section: Procedural Security

- **Finding:** The facility does not conduct a review of shipment information and documentation controls to verify accuracy and security.
No record was provided to demonstration that the factory conducted a review of shipment information and documentation controls to verify accuracy and security.
Recommendation: The facility must conduct a regular review of shipment information and documentation controls to verify accuracy and security.
- **Finding:** The facility does not consider company history, driver/employee hiring procedures, and existing transit security controls prior to selecting a highway transit carrier.
It was noted that prior to selecting a highway transit carrier, the facility did not consider company history, driver/employee hiring procedures, and existing transit security controls.
Recommendation: The facility must consider company history, driver/employee hiring procedures, and existing transit security controls prior to selecting a highway transit carrier.

Section: Information Security

- **Finding:** The facility does not have a written and implemented policy that designates which employees are permitted access to the information systems.
During this audit, it was noted that no "Restricted area" or authorized employees name list posted at information systems such as CCTV system.
Recommendation: The facility must have a written and implemented policy that designates which employees are permitted access to the information systems.
- **Finding:** System administrator does not receive a report of invalid password attempts.
It was noted that the system administrator did not receive a report of invalid password attempts per document review and management interview.
Recommendation: System administrator must receive a report of invalid password attempts.
- **Finding:** System administrator does not investigate reported incidents of attempted unauthorized system access or breach.
It was noted that the system administrator did not receive a report of invalid password attempts and could not provide with investigation records of reported incidents of attempted unauthorized system access or breach per document review and management interview.
Recommendation: System administrator must investigate reported incidents of attempted unauthorized system access or breach.
- **Finding:** The systems administrator does not regularly report a security incident to facility management.



It was noted that the factory established procedure for reporting security incident about information, but no reporting record was maintained in the factory. Factory management represented that they did not suffer any information incidents till now.

Recommendation: The systems administrator must report a security incident to facility management.



Facility Photos For Suzhou Fuyougang Can Products Co., Ltd

1.Facility Entrance



2.Perimeter Fencing



3.Facility Building



4.Employee Parking



5.Visitor Parking



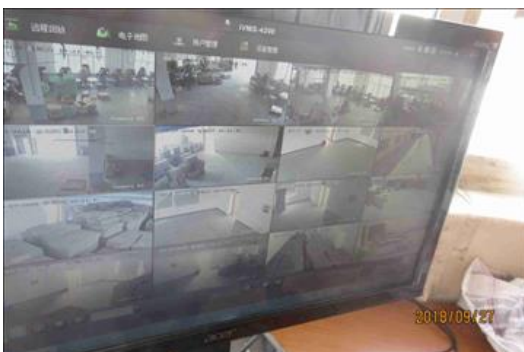
6.Outside Lighting



7.Security Room- Communication Equipment



8.CCTV system and monitor



9.Packing Area



10.Finished Goods Warehouse



11.Loading Area



12.Facility Name



DISCLAIMER

This report is for the exclusive use of the client of Bureau Veritas named in this report ("Client") and is provided pursuant to an agreement for services between Bureau Veritas and Client ("Client Agreement"). This report provides a summary of the findings and other applicable information found/gathered during the audit conducted at the specified facilities on the specified date only. Therefore, this report does not cover, and Bureau Veritas accepts no responsibility for, other locations that may be used in the supply chain of the relevant product or service. Further, as the audit process used by Bureau Veritas is a sampling exercise only, Bureau Veritas accepts no responsibility for any non-compliant issues that may be revealed relating to the operations of the identified facility at any other date. Bureau Veritas responsibility and liability are also limited in accordance to the terms and conditions of the Client Agreement. Bureau Veritas assumes no liability to any party, for any loss, expense or damage occasioned by the use of this information other than to the Client and in accordance with the Client Agreement and these disclaimers. The disclaimer should be read in conjunction with the Terms and Conditions of Bureau Veritas.