Embargoed till 25 May 2007, 12noon

SINGAPORE CUSTOMS

MEDIA RELEASE

SINGAPORE CUSTOMS UNVEILS THE SECURE TRADE PARTNERSHIP PROGRAMME (STP) TO MAINTAIN SINGAPORE AS A TRUSTED TRADE HUB

Singapore Customs unveils a new supply chain security programme for the trading community – **Secure Trade Partnership Programme** (STP) to strengthen and safeguard the security of supply chain operations. The Minister of State for Finance and Transport, Mrs Lim Hwee Hua, launched the STP at a ceremony on 25 May 2007. Eight companies have been certified under the STP after successfully completing the pilot-run of the programme.

About the STP

2 The STP is a voluntary certification programme administered by Singapore Customs that encourages companies to adopt robust security practices in their trading operations, thereby contributing to the improvement in the security of the global supply chain. Through the programme, Singapore Customs seeks to protect the integrity of the supply chain and prevent disruptions to the smooth flow of goods. The STP spells out a set of security guidelines and goals to guide the development, implementation, monitoring and review of the security measures by different players in the supply chain. These include suppliers, manufacturers, warehouse operators, transport carriers and terminal operators. Full details of the STP Guidelines are enclosed at Annex A.

3 Commenting at the launch of the STP, Mrs Lim Hwee Hua said, “In today’s global trading environment, it is not only important for Singapore to be efficient and well-connected, but also necessary to be secure and trusted. The Secure Trade Partnership Programme will help maintain Singapore’s position as a trusted trade hub.”

4 The Director-General of Customs, Mr Teo Eng Cheong, said “Every player in the trading community has a stake in a secure and resilient total supply chain. We would therefore like to see more companies certified as our STP Trusted Partners.”

5 Companies that apply for certification will have their internal policies, processes and procedures assessed against the STP Guidelines by Singapore Customs. The STP certification will serve as a testimony that companies have adequate internal security policies, processes and procedures to keep their supply chains secure. More information on the STP can be obtained in the enclosed information handbook (Annex B) or from the Singapore Customs website at www.customs.gov.sg.

Benefits of the STP

6 Companies that have adopted robust security measures will benefit from increased visibility of goods in the supply chain, reduction in pilferages and greater efficiency in their supply chain management.

7 In addition, companies certified under the STP will be recognised as trusted partners of Singapore Customs and enjoy the following benefits:

a) Cargo less likely to be inspected,
b) Recognition as a low risk company i.e. enhance branding, and
c) Reduced inspection/expedited clearance overseas should certified status be also recognised by overseas countries.

Companies Certified under STP

8 The pilot batch of eight companies which have been certified under the STP are as follows:

- APL Co. Pte Ltd
- Hewlett-Packard Asia Pacific Pte Ltd
- IBM Singapore Pte Ltd
- Infineon Technologies Asia Pacific Pte Ltd
- Poh Tiong Choon Logistics Limited
- PSA Corporation Limited
- United Parcel Service Singapore Pte Ltd
- YCH DistriPark (Pte) Ltd

Application

9 The STP is open for application to all companies in Singapore that are involved in supply chain activities. Application forms can be downloaded from Singapore Customs website at www.customs.gov.sg, or write in to Singapore Customs, 55 Newton Road #08-01, Revenue House, Singapore 307987, e-mail: customs_scs@customs.gov.sg or Fax: 62583705.

End of Release

ISSUED BY: **SINGAPORE CUSTOMS**
DATE: **25 MAY 2007**

Background of the STP

The establishment of Singapore's very own national supply chain programme was first announced by Deputy Prime Minister Professor S Jayakumar in a keynote address made at the *First APEC Symposium on Total Supply Chain Security* on 6 July 2006. Singapore Customs has been designated as the national authority for the STP. Its responsibilities include validating and certifying companies under the STP; serving as the focal point for all local and international enquiries; and conducting industry outreach and public awareness programmes on supply chain security.

SECURE TRADE PARTNERSHIP

SINGAPORE CUSTOMS

GUIDELINES

Contents

1 Introduction

1.1 The Secure Trade Partnership (STP) Guidelines spells out the requirements which companies in the supply chain should adopt to enhance the security of their operations and supply chains. Companies meeting such requirements will be certified as STP companies by Singapore Customs.

1.2 Under the STP Guidelines, companies are required to:

(a) have security management systems;
(b) conduct risk assessments of their business operations; and
(c) implement the security measures under the STP Guidelines to secure their supply chains.

1.3 The STP Guidelines provides companies with a framework to guide the development, implementation, monitoring and review of their supply chain security measures and practices.

1.4 Companies that decide to apply for certification under the STP will self-assess against the STP Guidelines to ensure that their internal policies, processes and procedures are robust.

2 Security Management System

2.1 Supply chain security can never be an isolated responsibility of a person or a unit operating within a company. To achieve a robust supply chain security implementation, security must be driven through a holistic company wide effort.

2.2 A company is required to establish a security management system to develop, document, implement, maintain and review the company's supply chain security measures and practices. The security management system should include but not be limited to:

(a) A framework for establishing and reviewing the company's security policy and objectives and commitment to security;

(b) A framework for effective communication within the company; and

(c) A review process to ensure continuing relevance and improvement.

3 Risk Assessment

3.1 The STP encourages companies to develop security profiles and implement security measures based upon a risk assessment of the companies' business models.

3.2 A company is required to conduct a risk assessment of its operational processes and supply chain. The company must seek to mitigate the risks and vulnerabilities of its operations within the supply chain.

Manufacturers/Suppliers

3.3 Manufacturers and suppliers are usually at the start of the supply chain for finished goods. Raw materials and products leaving their factories/plants have to be properly documented from the very onset so as to minimise exploitable data errors or the need for content verification at later stages of the chain. With accurate manifests, tamper-proof packaging, and well documented handing-over processes, manufacturers and suppliers will be able to hand over their goods to the cargo handling agents such as warehouse operators and transport companies in good shape for them to be moved through the supply chain securely.

Warehouse Operators and Owners

3.4 Warehouse operators and owners receive goods from manufacturers, transporters or other intermediaries, store them, and then provide them to other intermediaries, often in a different configuration. They should have a good information system to keep track of all the goods being handled and stored, and be able to provide the relevant information on the goods to the next intermediary in the chain. In addition, their premises should be appropriately secured to ensure that the goods trusted in their care are safe from tampering.

Transporters

3.5 Transport operators have a key responsibility in ferrying goods from one point to another. Transport operators should have measures to prevent their transport vehicles from being hijacked or substituted. They should also have a good information system to monitor and track the goods entrusted to them. In addition, transport operators should ensure that their vehicles and the goods being carried by their vehicles are not easily tampered with.

Terminal Operators

3.6 Terminal operators have a key responsibility for handling goods and containers prior to loading onto an aircraft or a vessel, and after unloading from an aircraft or a vessel. Essentially they are the last point before departure and first point on arrival for the goods and containers. Their premises should be appropriately secured to ensure that the goods and containers trusted in their care are safe from tampering.

Sea and Air Freight Operators

3.7 Sea and air freight operators have a key responsibility in ferrying goods from one point to another on vessels and aircrafts respectively. Sea and air freight operators should have measures to prevent their carriers from being hijacked or substituted while on their journeys. They should have a good information system to monitor and track the goods being entrusted to them. In addition, sea and air freight operators should ensure that their vessels and aircrafts and goods being carried on board their vessels and aircrafts are not easily tampered with.

4 Security Measures

4.1 The security measures under the STP Guidelines comprise 8 elements that a company must address:

(a) Premise security and access controls;
(b) Personnel security;
(c) Business partner security;
(d) Cargo security;
(e) Conveyance security;
(f) Information and Information Technology (IT) security;
(g) Incident management and investigations; and
(h) Crisis management and incident recovery.

4.2 The security measures adopted or implemented must seek to mitigate the risks and vulnerabilities identified from the company's risk assessment process.

4.3 Please refer to Appendix A for the Security Measures under the STP Guidelines.

Appendix A

STP Guidelines – Security Measures

1. Premise Security and Access Controls

Access controls and physical deterrents must be in place to prevent unauthorised access to the exterior and interior of companies' facilities. The system must include the positive identification of all employees and visitors at all points of entry.

1.1. Perimeter Fencing

Perimeter fencing and appropriate peripheral barriers should be in place to secure companies' premises. Perimeter fencing should enclose the yard or terminal, especially areas where container, cargo consignment, trailers and other rolling stock are parked or stored. All fencing should be regularly inspected for integrity and damage.

1.2. Gates and Gate Houses

Gates through which all vehicles and/or personnel enter or exit should be manned, monitored or otherwise controlled.

1.3. Parking

Parking access to facilities should be controlled and monitored. Private passenger vehicles should be prohibited from parking in close proximity to cargo handling and cargo storage areas.

1.4. Building Structure

Buildings should be constructed of materials that resist unlawful entry. The integrity of the structures should be maintained by periodic inspection and repair.

1.5. Locking Devices and Key Controls

All external and internal windows, doors, fences and gates should be secured with locking devices or alternative access monitoring or control measures. Management or security personnel should control the issuance of all locks and keys.

1.6. Lighting

Adequate lighting should be provided inside and outside companies' facilities including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

1.7. Alarm Systems and Video Surveillance Cameras

Alarm systems and video surveillance cameras should be utilised to deter potential intruders from attempting to gain entry, detect possible intrusion, expand the area of security surveillance, and assist in post-incident investigations.

1.8. Restricted Areas

Restricted areas should be clearly identified and monitored to prevent unauthorised access.

1.9. Security Personnel and Organisation

A personnel or unit should be in charge of the security of the company. Companies may engage the services of a security organisation to further enhance the security of their facilities.

1.10. Access Controls for Employees

An employee identification system should be in place for positive identification and access control purposes. For example, employees should be issued with colour photograph identification cards. Employees should only be given access to those areas needed for the performance of their duties.

1.11. Access Controls for Visitors

A visitor-identification and monitoring system should be in place. For example, visitors should present positive identification and register at the security station prior to entry into company premises and visitors should visibly display their temporary identification passes. All visitors should be escorted and only have access to those areas where they have legitimate business.

1.12. Challenging and Removing Unauthorised Persons

Procedures and training should be in place for all employees to report and challenge any unauthorised or unidentified persons.

2. Personnel Security

Procedures must be in place to screen prospective employees and to periodically check current employees. Procedures must be in place for educating and training of employees regarding security policies, recognition of deviations from those policies and understanding of what actions must be taken in response to security lapses.

2.1. Pre-Employment Verification, Background Checks and Investigations

Application information such as employment history, references, and educational records should be verified prior to employment.

Background checks and investigations should be conducted on prospective employees as appropriate and to the extent allowed under national law. Depending on the sensitivity of the job scope and/or job appointment that may compromise companies' operations, a more extensive background checks and investigations should be conducted on prospective employees.

2.2. Periodic Background Checks / Reinvestigations for Current Employees

Periodic checks and reinvestigations should be performed on current employees based on cause, and/or the sensitivity of employees' positions.

Companies should update information in individual personnel files, taking note of any unusual changes in their social and economic situations.

2.3. Education, Training and Awareness

Programmes should be in place to educate and train employees on security requirements including areas such as:

(a) The company's security policies;
(b) Recognising potential internal threats to security;
(c) Maintaining cargo integrity;
(d) Protecting access controls; and
(e) Identifying and reporting suspicious cargo, persons and activities.

Such programmes should be included into new employees' induction programme. A refresher course should be built into the programme to keep employees updated on current threats.

2.4. Termination Procedures

Procedures should be in place to expeditiously remove identification, premises and information systems access for employees whose employment has been terminated.

3. Business Partner Security

Companies must work with business partners and obtain their commitment to voluntarily increase their security measures, so as to bolster the security of the global supply chain.

The term "business partners" refers to current and prospective suppliers, manufacturers, service providers, contractors and vendors where companies outsource or contract elements of their supply chains.

3.1. Screening of Business Partners

Procedures should be in place for the screening, selecting, establishing and renewing of relationships with business partners. The procedures should include the conduct of interviews, reference checks and use of information provided by business partners and external resources. For example, business information services, banks and referrals from other organisations.

Screening and selection criteria such as legality, financial solvency and stability, ability to fulfil contractual security requirements, capability to identify and rectify security weaknesses where required may also be used.

3.2. Security Provisions in Agreements / Contracts or Security Declaration

Companies should include security provisions in written agreements and/or contracts with business partners or require business partners to provide a security declaration. The security provision or declaration should describe how goods are safeguarded, how associated information is protected, and how security measures are demonstrated and in place.

Agreements / contracts or security declarations should be reviewed when necessary and/or at least on a regular basis to suit companies' operations and changes in business environment.

3.3. Security Certification

Companies should obtain documentary proof of business partners' participation and certification by a foreign Customs Administration and/or other security programmes.

3.4. Review Business Partners' Adherence to Security Measures

Where appropriate, reviews should be conducted on business partners' processes and facilities to ascertain the validity of business partners' declarations on security. Where the findings are unsatisfactory, companies should communicate the issues to business partners and allow time for the issues to be rectified. Where necessary, companies may wish to reconsider their relationships with such business partners.

4. Cargo Security

Procedures must be in place to ensure that the integrity of cargo is maintained to protect against the introduction of unauthorised materials and/or persons.

4.1. Documentation Processing and Verification

Procedures should be in place to ensure that information in all documentation used in the movement and clearance of cargo, both electronic and manual, is legible, complete, accurate and protected against the exchange, loss or introduction of erroneous information. Companies should check for signs of tampering, forgery or other anomalies.

4.2. Receipt and Release of Cargo

Procedures should be in place to ensure that arriving and departing cargo is reconciled against relevant documents, for example, cargo manifest, packing list, bill of lading, purchase and delivery order. Procedures should be in place to check that cargo is accurately described, weighed, labelled, marked, counted and verified when receiving and releasing cargo. Persons / drivers delivering or receiving cargo should be positively identified before cargo is received or released.

4.3. Signature and Stamp Policies

Procedures should be in place on signature and stamp requirements for critical process handover points, for example, document preparation processes, issue of seals, breaking of seals, physical count of cargo, conveyance inspection, cargo delivery, cargo receipt and counting of unshipped pieces. Documents pertaining to custody and responsibility over cargo transferred or when a service is provided should be signed by the person delivering and receiving it.

4.4. Container Inspection

Procedures should be in place to verify the physical integrity of the container structure, including the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

(a) Front wall;
(b) Left side;
(c) Right side;
(d) Floor;
(e) Ceiling;
(f) Inside/outside doors; and
(g) Outside/undercarriage.

4.5. Seals and Markings

Procedures should be in place on how seals and markings are to be controlled, affixed and checked. The following measures are recommended:

(a) Only designated authorised person(s) should number and distribute seals and markings;
(b) A log should be kept to record the personnel receiving seals and markings and where they were used; and
(c) Seals and markings should not be issued in strict numbering sequence to avoid prediction of number.

Container seals should meet or exceed the current PAS ISO 17712 standards for high security seals.

4.6. Storage of Containers and Cargo

Containers and cargo should be stored in a secure area to prevent unauthorised access and/or tampering.

4.7. Inventory Control

Procedures should be in place to control the inventory and storage of cargo. The following measures are recommended:

(a) Stock-taking;
(b) Using trained watch service or warehouse staff to visually inspect inventory;
(c) Requiring step-by-step details of the checks and counter-checks performed by staff; and
(d) Requiring more frequent inspections during peak receiving period and discrepancy reporting.

5. Conveyance Security

Procedures must be in place to ensure that conveyances are capable of being effectively secured.

5.1. Conveyance Inspection

Procedures should be in place to ensure that potential places of concealment of illegal goods on conveyances are regularly inspected. All internal and external compartments and panels should be secured.

5.2. Tracking and Monitoring of Conveyance

Procedures should be in place to track and monitor accurately activities relating to the movement and handling of cargo both within companies' premises, and at handover points between companies and external parties. The tracking and monitoring system could be via:

(a) Electronic means. For example, transponders, smart cards, electronic seals, videos, digital photos, mobile phones, radios and Global Positioning Systems (GPS); or
(b) Activity logs etc.

5.3. Operators' Guide

Operators of conveyances should be trained to maintain the security of the conveyances and the cargo at all times and to report any actual or suspicious incident to designated security department staff. Guidelines should be in place to train operators on:

(a) Detail route planning for pick up and delivery;
(b) Confidentiality of load, route and destination;
(c) Policy on keys, parking area, refuelling and unscheduled stops;
(d) Reporting for accident or emergency;
(e) Reporting of any irregularity in loading, locking and sealing; and
(f) Installation and testing of security alarms and tracking devices, if any.

5.4. Storage of Conveyance

Conveyances should be stored in a secure area to prevent unauthorised access and/or tampering.

6. Information and Information Technology (IT) Security

Procedures must be in place to maintain confidentiality and integrity of data (physical and electronic) and information systems used in the supply chain including protection against misuse and unauthorised alteration.

6.1. Information Security Policy

An information security policy and procedures and/or security-related controls such as firewalls, passwords, anti-virus software and encryption software, etc, should be in place to protect information systems from unauthorised access.

6.2. Information/Document Classification, Handling and Access Controls

Procedures should be in place for classifying information/documents according to their sensitivity and criticality. Important and sensitive information and documents should be stored in a secure area or system which is accessible only to authorised personnel. Regular reviews should be conducted to ensure that rights and privileges granted are appropriate and have not been abused.

6.3. Data Life Cycle Control

Procedures should be in place to control the life cycle of data.

6.4. Data Back-ups and Recovery Plans

Procedures and back-up capabilities should be in place to protect against the loss of information.

7. Incident Management and Investigations

Procedures must be in place to provide a coordinated, structured and comprehensive response to an incident or risk situation and identify root causes so that actions can be taken to prevent recurrences.

7.1. Reporting Incidents

Procedures should be in place for reporting incidents such as shortages and over landing of cargo, irregularity or illegal activities and security breaches to management.

Companies should maintain a database of incident reports, actively monitor and identify trends and patterns for potential security risks and breaches.

7.2. Investigate and Analyse

Procedures should be in place to ensure that incidents are investigated and analysed with the objectives of determining the cause of the incident and implementing the necessary revisions and improvements to prevent the recurrence of such an incident.

8. Crisis Management and Incident Recovery

In order to minimise the impact of a disaster or security incident, crisis management and recovery procedures should be in place. The procedures should include advance planning and establishment of processes to operate under such extraordinary circumstances.

8.1. Contingency or Emergency Plans

Contingency or emergency plans for disaster or emergency security situations should be in place.

The contingency or emergency plans should be communicated to all appropriate employees and regularly updated as operational and organisational changes occur. Companies should conduct periodic training of employees and testing of contingency or emergency plans.

8.2. Business Continuity Plan (BCP)

Companies are encouraged to develop a Business Continuity Plan (BCP) to ensure that Critical Business Functions (CBF) can continue during and after a crisis or disaster affecting their companies or segments of their supply chains.

CONTACT US

For more information on the STP,

please visit our website at www.customs.gov.sg or

email us at customs_scs@customs.gov.sg

Supply Chain Security Branch

Singapore Customs

55 Newton Road #08-01

Revenue House

Singapore 307987

Singapore Customs

Handbook on Secure Trade Partnership (STP)

SINGAPORE CUSTOMS

Preface

International trade is one of the key drivers of global economic growth. In today's globalised world, cargo supply chains are highly interconnected, complex and involve multiple players.

The ever-increasing complexity of the global supply chain also means more vulnerability to threats such as thefts, pilferages and terrorist attacks. It would be most unfortunate should the global trading system be disrupted by a single act of crime or terror anywhere along the supply chain.

Total supply chain security can only be achieved if every player along the entire supply chain, right from the point of origin to the point of final destination, takes responsibility in securing his part of the supply chain. To fulfill this objective, many countries have implemented or are implementing their national supply chain security initiatives.

As a key player in the global supply chain, Singapore has implemented the Secure Trade Partnership (STP) programme in partnership with our businesses to help raise the overall level of supply chain security standards in Singapore. The STP will ensure that we are not just an efficient and connected port, but also a safe and secure trading hub.

Contents

1 About This Handbook

1.1 Is this handbook meant for me?

1.1.1 If you wish to have your company certified under the Secure Trade Partnership (STP) programme, you should read this handbook.

1.2 What is this handbook about?

This handbook provides you with information on:

(a) How the STP programme works; (Please refer to Section 2.)

(b) The requirements under the STP Guidelines; (Please refer to Section 3.)

(c) How to apply for the STP; (Please refer to Section 4.)

(d) What is a STP validation; (Please refer to Section 5.)

(e) Certification under the STP; (Please refer to Section 6.) and

(f) Other information. (Please refer to Section 7.)

2 Overview of the Secure Trade Partnership (STP)

2.1 What is Secure Trade Partnership (STP)?

2.1.1 Launched on 25 May 2007, the STP is a voluntary certification programme administered by Singapore Customs to help companies adopt robust security measures to enhance the security of the global supply chain.

2.1.2 The STP Guidelines spells out the requirements which companies in the supply chain should adopt to enhance the security of their operations and supply chains. Companies meeting such requirements will be certified as STP companies by Singapore Customs.

2.1.3 The STP is consistent with the World Customs Organisation (WCO) SAFE Framework of Standards to secure and facilitate global trade, adopted in June 2005.

2.2 How does the Secure Trade Partnership (STP) work?

2.2.1 By participating in the STP, companies will be demonstrating their commitment to adopt and implement appropriate security measures and their willingness to assume responsibility for keeping their supply chains secure.

2.2.2 Companies that decide to apply for certification under the STP will first need to self-assess against the STP Guidelines to ensure that their internal policies, processes and procedures are robust.

2.2.3 Singapore Customs administers a validation and certification process to certify companies that wish to participate in the STP.

2.2.4 The STP application and certification process involves:

(a) A company performing a comprehensive self-assessment of its internal policies, processes and procedures against the STP Guidelines. The result of the self-assessment would be the formulation of the company's security profile that covers the following:
   (i) The company's security management system;
   (ii) The company's risk assessment process;
   (iii) The company's security measures that address the 8 security elements under the STP Guidelines:
      (1) Premise security and access controls;
      (2) Personnel security;
      (3) Business partner security;
      (4) Cargo security;
      (5) Conveyance security;
      (6) Information and Information Technology (IT) security;
      (7) Incident management and investigations; and
      (8) Crisis management and incident recovery.

   Please refer to Section 3 for an Overview of the STP Guidelines;

(b) The company submitting an application to Singapore Customs, together with its security profile and supporting documents. Please refer to Section 4 for more details on the application to the STP;

(c) Singapore Customs assessing the company's application and security profile for compliance with the STP Guidelines. The assessment will include on-site validation(s) by Singapore Customs. Please refer to Section 5 for more details on the on-site validation; and

(d) Singapore Customs certifying the company if it meets the requirements under the STP Guidelines.

2.2.5 The STP certification will be valid for a period of 3 years. Certified companies have to comply with the terms and conditions stipulated by Singapore Customs. Singapore Customs will conduct periodic and regular site visits. Please refer to Section 6 for more details on certification under the STP.

2.3 Who can apply for the Secure Trade Partnership (STP)?

2.3.1 The STP is open to companies in Singapore that are involved in supply chain activities. Companies which believe that they can meet the requirements under the STP Guidelines can apply to join the STP.

2.3.2 In reviewing an application from a company, Singapore Customs will consider the following:

(a) The company's compliance history with Singapore Customs and other relevant government authorities;

(b) The company's security measures and standards; and

(c) Related information on the company from local and/or foreign government authorities, where appropriate.

2.4 Why would a company want to be part of the Secure Trade Partnership (STP)?

2.4.1 A company that is certified under the STP will be recognised as a trusted partner of Singapore Customs and will partner Singapore Customs to enhance the security of the global supply chain.

2.5 What are the benefits of joining the Secure Trade Partnership (STP)?

2.5.1 Companies that have adopted and implemented robust security measures will benefit from increased visibility of goods in the supply chain, reduction in pilferages and greater efficiency in their supply chain management.

2.5.2 In addition, companies certified under the STP will be recognised as trusted partners of Singapore Customs and enjoy the following benefits:

(a) Cargo less likely to be inspected;

(b) Recognition as a low risk company i.e. enhanced branding; and

(c) Reduced inspection or expedited clearance should certified status be also recognised by overseas countries.

2.6 Will the Secure Trade Partnership (STP) Guidelines apply equally to companies of all sizes?

2.6.1 Yes. Business operation models, sizes and risks vary across the different nodes in the supply chain and across different industries. The STP recognises these and allows for flexibility and customisation of security profiles based on companies' business models.

2.7 Will participation in other security programmes affect a company's obligation to comply with the requirements under the Secure Trade Partnership (STP) Guidelines?

2.7.1 The STP recognises that companies may have already undertaken security measures on their own accord to strengthen their internal security systems, or may have already participated and implemented measures under other security programmes. It is not the intention of the STP to replace or supersede a company's existing security systems or measures. The STP seeks to build upon industry best practices and partnerships to strengthen the security of the global supply chain.

2.7.2 The various security programmes have slightly different objectives and hence, they will not be direct substitutes for the STP. Existing certifications that a company already complies with will be taken into account, if the security requirements are comparable to those required under the STP Guidelines.

3 Overview of the Secure Trade Partnership (STP) Guidelines

3.1 What is the Secure Trade Partnership (STP) Guidelines?

3.1.1 The STP Guidelines spells out the requirements which companies in the supply chain should adopt to enhance the security of their operations and supply chains. Companies meeting such requirements will be certified as STP companies by Singapore Customs.

3.1.2 Under the STP Guidelines, companies are required to:

(a) Have security management systems;
(b) Conduct risk assessments of their business operations; and
(c) Implement the stipulated security measures under the STP Guidelines to secure their supply chains.

3.1.3 The STP Guidelines provides companies with a framework to guide the development, implementation, monitoring and review of their security measures and practices.

3.1.4 For more details, please refer to the STP Guidelines on Customs website (http://www.customs.gov.sg/).

3.2 What is the security management system?

3.2.1 Supply chain security can never be an isolated responsibility of a person or a unit operating within a company. To achieve a robust supply chain security implementation, security must be driven through a holistic company wide effort. Companies must establish security management systems to develop, document, implement, maintain and review the companies' security measures and practices. The security management system should include but not be limited to:

(a) A framework for establishing and reviewing the company's security policy and objectives and commitment to security;

(b) A framework for effective communication within the company; and

(c) A review process to ensure continuing relevance and improvement.

3.3 Why is the risk assessment process necessary?

3.3.1 The STP encourages companies to develop security profiles and implement security measures based upon risk assessments of their business models. Companies must conduct risk assessments of their operational processes and supply chains.

3.3.2 Companies must seek to mitigate the identified risks and vulnerabilities of their operations within the supply chains.

3.4 What are the security measures' requirements?

3.4.1 The security measures under the STP Guidelines comprise 8 security elements that companies must address:

(a) Premise security and access controls;
(b) Personnel security;
(c) Business partner security;
(d) Cargo security;
(e) Conveyance security;
(f) Information and Information Technology (IT) security;
(g) Incident management and investigations; and
(h) Crisis management and incident recovery.

3.4.2 The security measures adopted or implemented must seek to mitigate the risks and vulnerabilities identified from the company's risk assessment process.

3.4.3 For more details, please refer to the STP Guidelines on Customs website (http://www.customs.gov.sg/).

4 Application for the Secure Trade Partnership (STP)

4.1 What information should be provided when a company applies for the Secure Trade Partnership (STP)?

4.1.1 The information to be submitted in a company's application should include:

(a) Application Form for the STP. Please refer to Customs website (http://www.customs.gov.sg/) for the application form;

(b) An introduction of the company;

(c) The company's security profile which comprises the following:

(i) A summary of the company's security management system;
(ii) A summary of the company's risk assessment process; and
(iii) Security measures put in place by the company to enhance the security of the company's supply chain.

Please refer to the Guide for Completing Security Profile on Customs website (http://www.customs.gov.sg/).

(d) Supporting documents which include:

(j) Process map(s) that illustrates the flow of goods and documentation/information through the company's supply chain. Please refer to Appendix A for the Factsheet on Company's Process Map.

(ii) Site plan(s) that shows the layout of the company's premises and clearly identifies all perimeters, access areas, buildings, structures, security and access controls. Please refer to Appendix B for the Fact Sheet on Company's Site Plan.

(e) Copy of the company's relevant security accreditations; and

(f) Any other relevant supporting documents.

4.2 What information should be provided for the introduction of a company?

4.2.1 The introduction of a company should contain the following information:

(a) The background and history of the company;
(b) The company's principal operations;
(c) Products that the company is dealing with;
(d) The company's organisation chart and number of employees;
(e) The company's relevant security accreditations; and
(f) Any other relevant information.

4.3 What information should be provided for the summary of a company's management system?

4.3.1 The summary of a company's security management system should contain the following information:

(a) The company's security policy, security objectives and commitment to security;

(b) The procedures for ensuring that pertinent security management information is communicated to and from relevant employees and other stakeholders;

(c) The procedures for the review of the company's security profile at planned intervals, to ensure its continuing suitability, adequacy and effectiveness; and

(d) Any other relevant information.

4.4 What information should be provided for the summary of a company's risk assessment?

4.4.1 The summary of a company's risk assessment should contain the following information:

(a) A flow chart to illustrate the company's risk assessment process;

(b) The risks and vulnerabilities identified from the company's risk assessment process;

(c) The countermeasures put in place to reduce the identified risks and vulnerabilities;

(d) When the risk assessment was conducted;

(a) Who conducted the risk assessment; and

(b) Any other relevant information.

4.5 Does a company need to engage a consultant to assist in the conduct of the company's risk assessment?

4.5.1 It is not a requirement under the STP for a company to engage a consultant to assist in the company's risk assessment. It is the company's decision whether to engage a consultant.

4.6 What is the level of details to be provided in a company's security profile?

4.6.1 A company should provide as much information as possible in its security profile, making references to supporting documents such as standard operating procedures which can be attached together with the STP application. This will allow Singapore Customs to be more familiar with and to obtain a better understanding of the security measures put in place by the company.

4.7 What if one of the security measures does not apply to my company?

4.7.1 The STP recognises the complexity of international supply chains and allows for flexibility and customisation of security profiles based on companies' business models. If one of the security measures does not apply to your company, please explain why. If your company adopts measures that are different from those in the STP Guidelines, please document them in your security profile.

4.8 Can I use reference to describe my company's security measures?

4.8.1 Yes. You can use references such as standard operating procedures for the security measures, provided this is prefaced with a short description. The standard operating procedures can be attached together with the STP application.

4.9 Do I need to cover all sites in my company's security profile?

4.9.1 Yes. The security profile must cover all your company's sites. Where operations at any of these sites are considerably different, your company should develop separate assessments and security profiles for each type of operation.

4.10 Are there terms and conditions for application to the Secure Trade Partnership (STP)?

4.10.1 Yes, please read the terms and conditions stipulated in the Application Form for the STP.

4.11 Do I need to submit security profiles of my company's business partners?

4.11.1 You are not required to submit security profiles of your business partners when you submit your company's STP application.

4.11.2 However, Singapore Customs may request for information/documents related to the elements of your company's supply chain that are outsourced or contracted to your business partner. The officer who processes the application will advise on the information/documents requirements, where appropriate.

4.12 How do I apply?

4.12.1 To apply for the STP, please send your completed STP application to Singapore Customs:

(a) Via email to customs_scs@customs.gov.sg; or

(b) Via fax to 6258 3705; or

(c) By mail to Singapore Customs, 55 Newton Road, #08-01, Revenue House, Singapore 307987. Attention to Supply Chain Security Branch.

4.13 How long will the application process take?

4.13.1 The duration of the application process will depend on the complexity of a company's business operations and the number of sites. The officer who receives the company's application will be able to provide an indication of the timeframe.

4.14 How much will the application cost?

4.14.1 There is no application fee.

5 Validation

5.1 What is a validation under the Secure Trade Partnership (STP)?

5.1.1 A validation is a process by which Singapore Customs visits a company to verify that the information outlined in the company's security profile is accurate and implemented.

5.1.2 The validation visit also serves as a platform for Singapore Customs and the company to build up a partnership of trust and to develop a better understanding of each other.

5.2 Will all companies that decide to participate in the Secure Trade Partnership (STP) undergo a validation?

5.2.1 Yes. All companies that decide to participate in the STP will have to be validated by Singapore Customs before they are certified under the STP.

5.3 Who will conduct the validation?

5.3.1 Singapore Customs will conduct the validation.

5.4 What is expected of a company during a validation?

5.4.1 The company must have all relevant documents/information available for review during the validation. The company must arrange for a tour of the company's site(s) and have company representatives available during the validation to address the following:

(a) Overview of the company;
(b) The company's security management system;
(c) The company's risk assessment process; and
(d) The company's security measures addressing the following 8 security elements:
    (i) Premise security and access controls;
    (ii) Personnel security;
    (iii) Business partner security;
    (iv) Cargo security;
    (v) Conveyance security;
    (vi) Information and Information Technology (IT) security;
    (vii) Incident management and investigations; and
    (viii) Crisis management and incident recovery.

5.5 Will Singapore Customs conduct validations at all the company's sites?

5.5.1 Yes. Singapore Customs will conduct validations at all the company's sites.

5.6 Will Singapore Customs conduct validation on a company's business partners?

5.6.1 Singapore Customs may conduct selective validations on the company's key business partners. The officer who processes the company's STP application will advise on the validation requirements, where appropriate.

5.7 Will Singapore Customs conduct overseas validation?

5.7.1 Singapore Customs will not conduct overseas validation.

5.8 How will validation findings impact a company's participation in the Secure Trade Partnership (STP)?

5.8.1 If the validation findings are satisfactory, the company will be certified as an STP company.

5.8.2 If the validation findings reveal significant weaknesses in the company's security profile, Singapore Customs will reject the application or work with the company to develop a work plan to rectify the areas of weakness.

5.9 Will validation findings be communicated to a company?

5.9.1 Yes. Singapore Customs will communicate the validation findings to the company.

5.10 How long will the validation process take?

5.10.1 The duration of the validation process will depend on the complexity of a company's business operations and the number of sites that the company has. The officer who processes the company's application will be able to provide an indication of the timeframe.

6 Certification under the Secure Trade Partnership (STP)

6.1 What are responsibilities of a Secure Trade Partnership (STP) company?

6.1.1 In addition to the responsibilities stated in the Application Form, an STP company's responsibilities include:

(a) To update Singapore Customs as and when there are significant changes to the company's security profile;

(b) To submit an annual statement of commitment on the anniversary dates of the company's STP certification; and

(c) To inform Singapore Customs of any non-conformities by the company with STP Guidelines.

6.2 Will Singapore Customs conduct site visits to an STP company during the 3-year certification period?

6.2.1 Yes. Singapore Customs will conduct periodic and regular site visits. Singapore Customs will provide notice to the STP company prior to the site visits.

6.3 Will there be any penalties imposed on an STP company for non-compliance to the terms and conditions?

6.3.1 Non-compliance to the terms and conditions of the STP certification will result in suspension or removal of a company's certification status and associated benefits.

6.4 When will a company's STP status be suspended?

6.4.1 A company can have its STP certification suspended if:

(a) The company does not abide by the terms and conditions of the STP certification; or

(b) There is non-compliance by the company with Singapore Customs laws and regulations and/or with the laws and regulations of other relevant Singapore government authorities; or

(c) Supply chain security weaknesses in the company or non-conformity by the company with STP Guidelines are discovered and not rectified to Singapore Customs' satisfaction.

6.4.2 Once suspended, the company will lose its STP status and associated benefits. The company will have its STP status and associated benefits re-instated when the areas of weakness or non-compliance are rectified to the satisfaction of Singapore Customs.

6.4.3 If the company is unable to take the required measures to rectify the areas of weakness or non-compliance to the satisfaction of Singapore Customs within a stipulated period of time, the company will have its STP status and associated benefits removed.

6.5 When will a company's STP status be removed?

6.5.1 A company can have its STP certification status removed if:

(a) The company does not abide by the terms and conditions of the STP certification; or

(b) There is serious non-compliance by the company with Singapore Customs laws and regulations and/or with the laws and regulations of other relevant Singapore government authorities; or

(c) Serious supply chain security weaknesses in the company or non-conformity by the company with STP Guidelines are discovered and not rectified to Singapore Customs' satisfaction.

6.5.2 The company will have its STP status and associated benefits removed immediately.

6.5.3 After removal, the company cannot re-apply for STP certification within 1 year.

6.6 Can an STP company withdraw from the Secure Trade Partnership (STP)?

6.6.1 Yes. The STP is a voluntary programme and an STP company is able to withdraw from the STP if it no longer wishes to be in the programme. The company has to write in to lodge its request with Singapore Customs. Upon withdrawal, the company will have its STP status and associated benefits removed.

6.7 Can a company's STP status be renewed?

6.7.1 Yes. A company can renew its STP certification if it wishes to continue to participate in the STP.

7 Other Information

7.1 Who will have access to business documents/information provided in companies' applications?

7.1.1 The business documents/information are for Singapore Customs' purposes only and will not be disclosed to a third party without the companies' prior written consent. All business documents/information provided by the companies will remain confidential.

7.2 Is there an appeal process within the STP programme?

7.2.1 A company can lodge an appeal against a decision of Singapore Customs made with regards to the company's application and participation in the STP programme. The company has to write in to lodge its appeal with Singapore Customs within 28 days from the date of the relevant decision communicated to the company by Singapore Customs.

7.3 Contact information

7.3.1 This handbook is developed to provide a general overview of the STP programme. Should you need further clarifications or advice, please contact our Supply Chain Security Officers:

(a) Via email to customs_scs@customs.gov.sg; or

(b) Via fax to 6258 3705; or

(c) By mail to Singapore Customs, 55 Newton Road, #08-01, Revenue House, Singapore 307987. Attention to Supply Chain Security Branch.

Appendix A

Fact Sheet on Company's Process Map

1 What is a process map?

1.1 A process map illustrates the flow of goods and documentation/information through a company's supply chain.

2 Why is the process map necessary?

2.1 The process map allows Singapore Customs to see the continuous link of activities that take place within a company's supply chain and provides us with a better understanding of the company's entire supply chain.

3 What information must the process map contain?

3.1 The process map must cover a company's entire supply chain, accounting for both the physical and documentary processes.

4 What if a company has multiple sites with different operations?

4.1 If a company has multiple sites and operations at any of these sites are considerably different, the company should develop separate process maps for each type of operation.

5 If a company has many different products that undergo different logistics routes and supply chain processes (i.e. process maps), does the company need to provide a process map for each product?

5.1 If there are many different supply chain processes, a company can provide a general process map that shows the different activities involved at each stage. Singapore Customs will request for detailed process maps, if necessary. If a general process map is not feasible, the processes should be separately mapped.

5.2 An example of a basic process map is attached to assist you.

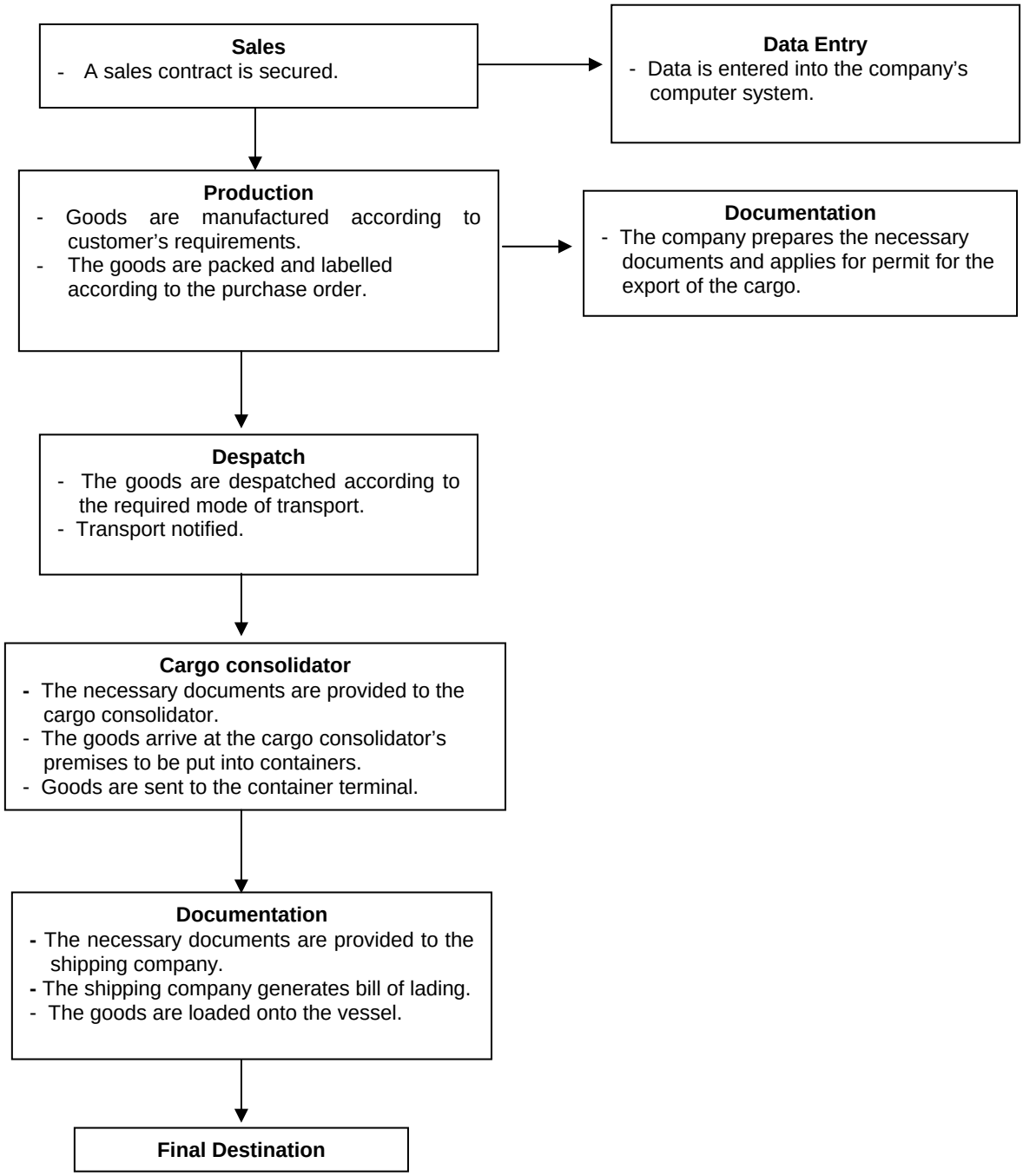
An Example of a Process Map

Name of company:

Dated:

Name of site:

Type of operation:



Appendix B

Fact Sheet on Company's Site Plan

1 What is a site plan?

1.1 A site plan shows the layout of a company's premises and clearly identifies all perimeters, access areas, buildings, structures, security and access controls.

2 Why is the site plan necessary?

2.1 The site plan provides Singapore Customs with an overview of the environment where a company operates and the security features on-site to enhance the security of the company's operations.

3 What information must the site plan contain? How detailed must the site plan be?

3.1 The site plan must be to scale and clearly identify a company's site boundaries, the various buildings within the site and also the usage of any open areas. Entry points to the site and the buildings within the site must be clearly indicated and labeled. The company should also preferably include in the site plan the positions of lightings (flood lights, emergency lights etc), CCTVs (coverage) and any other security equipment in the company's premises. The site plan must be dated and identified with the name and address of the site.

4 What if a company has multiple sites?

4.1 If a company has multiple sites and the layouts at any of these sites are considerably different, the company should develop separate site plans for each site.