C-TPAT Requirements

January 2016

C-TPAT Framework

- "Best Practices" are defined as:
  1. Security measures that exceed C-TPAT Security Criteria,
  2. Incorporate high-level management support,
  3. Have written policies and procedures that govern their use,
  4. Employs a system of checks and balances, and
  5. Have measures in place to ensure continuity.
- Flexible approach: "One Size does not fit all". Customized security measures must be developed and implemented in accordance with the risk present.
  - Adoption of certain best practices in a low risk environment may be sufficient to mitigate the risk present and enable the importer to qualify for Tier Three standing. However, in a high-risk environment, the adoption of the same practices may not elevate the security environment to qualify the importer as Tier Three.
- Tiered Benefit Structure
  - In 2005, CBP moved to a three-tiered benefits structure, where C-TPAT importers who do more, receive more.

MAGUSA LOGISTICS

The Application Process

- Participants complete an online electronic application on www.cbp.gov that includes submission of:

  - Corporate information

  - Supply chain security profile, which encompasses following areas:
    - Business Partner Requirements
    - Procedural Security
    - Physical Security
    - Personnel Security
    - Education and Training
    - Access Controls
    - Manifest Procedures
    - Information Security, and
    - Conveyance Security.

  - Acknowledgement of an agreement to voluntarily participate.

- Upon satisfactory completion of application and supply chain security profile, participants are assigned a CBP C-TPAT Supply Chain Security Specialist (SCSS), who will contact the participant to begin the validation process.

MAGUSA LOGISTICS

C-TPAT Validation Process

- Validation is a process through which US Customs and Border Protection (CBP) meets with program participant representatives, and visits selected domestic and foreign sites, to verify that the supply chain security measures contained in the C-TPAT participant's security profile are accurate and being followed.

- Validation should not be more than 10 working days. CBP will provide 30 days advance notice prior to the beginning of any validation.

- At the conclusion of validation, company management will be briefed on the findings of the validation. A written report will be presented to the company shortly thereafter.

MAGUSA LOGISTICS

C-TPAT Security Link Portal

- Allows participant to:
  - Enter new applications
  - Instantly submit information updates and add new information
  - Maintain a “living” Supply Chain Security Profile that can be updated as needed and must be updated and re-certified on a yearly basis
  - Communicate directly with CBP C-TPAT and/or their designated SCSS using a secure system.
  - Receive information directly from CBP to include cargo security alerts and sanitized intelligence information.
  - Maintain a list of authorized users.

MAGUSA LOGISTICS

Corporate Governance Structure Supporting Supply Chain Security

- Tier Three Status can only be obtained by the presence of this practice.
- Supply Chain security is embraced at highest levels of the company – CEO, COO, the President, etc.
- The security of Supply Chain should be a required topic of discussions in corporate boardrooms.
- Security practices must be periodically reviewed for adequacy by CEOs and corporate boards, and noted deficiencies must be addressed timely.
- Security best practices should become an integral part of a company's culture by being incorporated into the company's mission and core business processes.

MAGUSA LOGISTICS

Security Guidelines for Air Freight Consolidators, Ocean Transportation Intermediaries and NVOCCs.

- Consolidators must conduct a comprehensive assessment of their international supply chains.
- Where the consolidator outsources, then it must work with business partners to ensure that security measures are in place and adhered to.
- The supply chain for C-TPAT purposes is defined from point of origin through the point of distribution.
- C-TPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based on risk analysis. Therefore, the program allows for flexibility and the customization of security plans based on the member's business model.

MAGUSA LOGISTICS

Risk Analysis

- Given the complexity of the international supply chain, a risk analysis is necessary to focus resources and prioritize action items.
- Helps to identify and address the most immediate threat(s) to their supply chain
  - Research terrorist/criminal activity in supplier countries.
  - Conduct security surveys to all foreign suppliers and service providers.
  - Develop an action plan to address the gaps, vulnerabilities and weaknesses in security.
- Risk analysis requires constant communication with business partners and knowledge about their security measures.
- Tapping Into Existing Resources. CBP or the U.S. Department of State web sites on a regular basis determine what cargo is of moderate or high risk for smuggling, sabotage or terrorist attack.

MAGUSA LOGISTICS

Self-Assessment

- Self-Assessment enable companies to evaluate the effectiveness of the security measures used within their international supply chain. In addition, helps to identify the need for additional resources, as well as correct gaps, vulnerabilities, and weaknesses.
- Domestic Facilities.
  - Audit security procedures, equipment, training and other asset protection measures. Includes auditing container inspections reports.
  - Company incorporated supply chain security into its internal management audits.
  - Verifying/Rotating Security Guard Duties.
  - Verifying Physical Security. Daily inspections of alarms, surveillance camera systems, and access control devices are working, and that fence lines are maintained.
- Foreign Facilities.
  - Holding Partners Accountable. Company will conduct several unannounced on-site security inspections of its suppliers and service providers. Company amend contracts with partners to include minimum-security requirements and risk-based audits.
  - Utilizing External Resources. Hiring a security firm to physically verify that security criteria is met by partners, as agreed.

MAGUSA LOGISTICS

Business Partner Requirement

- Importers must have written and verifiable processes for the selection of business partners including foreign consolidators, customers, contractors, cargo handling, carriers, and vendors.

- Must ensure that contracted providers adopt C-TPAT guidelines.

- Periodically review performance of these providers.

MAGUSA LOGISTICS

Security Procedures

- Point of Origin
  - Consolidators must ensure business partners develop processes consistent with C-TPAT guidelines to enhance integrity of the shipment at the point of origin. Periodic reviews of processes and facilities should be conducted based on risk.

- Participation/Certification in Foreign Customs Administrations Supply Chain Security Programs
  - Current or prospective business partners should indicate status if have obtained certification with other customs agencies.

- Service Provider Screening and Selection Procedures
  - Consolidator should have documented service provider screening and selection procedures to screen the contracted service provider for validity, and the ability to identify and correct security deficiencies as needed. Service Provider procedures should utilize a risk-based process as determined by an internal management team.

- Customer Screening Procedures
  - Consolidator should have documented procedures to screen prospective customers for validity, financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed. Customer screening procedures should utilize a risk-based process as determined by an internal management team.

MAGUSA LOGISTICS

Container Security

- Consolidators should ensure that all contracted service providers have procedures in place to maintain container security.
- Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons.
- At point of stuffing, procedures must be in place to properly seal and maintain integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for the U.S. Seals are to exceed PAS ISO 17712 standards. Must use “H” type.
- Container Inspection. Procedure must be in place to verify physical integrity of the container prior to stuffing (including locking mechanisms at doors). A seven-point inspection is recommended: front wall, left side, right side, floor, ceiling/roof, inside/outside doors, outside/undercarriage.
- Container Seals. Written procedures must stipulate how seals are to be controlled and affixed to loaded containers to include procedures for recognizing and reporting compromised seals to US Customs and Border or foreign authorities. Seal verification and inspection process should be used before seals are put in place and closed. Only designated employees should distribute container seals.
- Container Storage. Containers must be stored in a secure area. Procedures should be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

MAGUSA LOGISTICS

Physical Access Controls

- Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors and protect company assets. Must include the positive identification of all employees, visitors and vendors at all points of entry.
- Employees. An employee identification system must be in place for positive identification and access control purposes. Selected access are given by employee. Management must control issuance and removal of employee, visitor and vendor identification badges. Procedures for issuance and removal and changing access devices must be documented.
- Visitor Controls. Visitors must present photo ID upon arrival. All visitor should be escorted and visibly display temporary identification.
- Deliveries (including mail). Proper vendor ID must be presented for identification upon arrival by all vendors. Arriving packages should be periodically screened before being disseminated.
- Challenging and Reporting Unauthorized Persons. Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

MAGUSA LOGISTICS

Personnel Security

- Processes must be in place to screen prospective employees and to periodically check current employees. Maintain an updated permanent employee list (foreign and domestic), which includes the name, date of birth, national ID or social security number, position held and submit such information to CBP upon written request, to the extent permitted by law.
- Pre-Employment Verification. Application information, such as employment history and references must be verified prior to employment.
- Background Checks/Investigations. Consistent with foreign, federal, state and local regulations, background checks and investigation should be conducted for prospective employees. Periodic checks and reinvestigations should be performed based on cause and/or the sensitivity of the employee's position.
- Personnel Termination Procedures. Companies must have procedures in place to remove identification; facility and system access for terminated employees.

MAGUSA LOGISTICS

Procedural Security

- Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in the supply chain.
- Regardless of a company's size, written policies are needed. Procedural security requires oversight, accountability, control, and a system of checks and balances.
- Documentation Processing. Procedures must be in place to ensure that all documentation used in the movement of cargo is legible, complete, accurate and protected against exchange, loss or introduction of erroneous information. It must include safeguarding computer access and information.
- At the time of container stuffing, a shipping supervisor and security guard are present, each have back ups when absent. Responsible parties should sign-off "check sheet".
- Manifesting Procedures. Procedures must be in place to ensure that information received from business partners is reported accurately and timely. A detailed Standard Operating Procedure (SOP) exists between the Freight Forwarder and the Shipper.
- Shipping & Receiving. Arriving cargo should be reconciled against information on the cargo manifest. Cargo should be accurately described, weighed, labeled, marked, counted and verified.
- Cargo Discrepancies. All shortages, overages and other significant discrepancies must be resolved and/or investigated appropriately. CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

MAGUSA LOGISTICS

Security Training and Threat Awareness

- A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain.
- Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.
- Specific training should be offered to assist employees in the maintaining cargo integrity, recognizing internal conspiracies and protecting access controls.
- These programs should offer incentives for active employee participation.

MAGUSA LOGISTICS

Physical Security

- Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.
- Fencing/Gates. Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing should segregate domestic, international, high value and hazardous cargo. Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary.
- Security Guards. Guards are equipped with adequate resources. Guards are rotated.
- Parking. Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.
- Building Structure. The integrity of the structures must be maintained by periodic inspection and repair.
- Locking Devices and Key Controls. All external and internal windows, gates and fences must be secured with locking devices. Management must control issuance of locks/keys.
- Lighting. Adequate lighting must be provided inside and outside the facility. Including: entrances and exits, cargo handling, storage areas, fence lines and parking areas.
- Alarm Systems & Video Surveillance Cameras. Should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

MAGUSA LOGISTICS

Information Technology Security

- IT integrity must be maintained to protect data from unauthorized access or manipulation.
- Password Protection. Systems must use individually assigned accounts that require a periodic change of password (at least every 90 days). IT security policies, procedures and standards must be in place and provided to employees in the form of training.
- Access Levels. Levels of access to the computer system are assigned by job category and established by the corporate office. Management periodically evaluates access levels or current users and will change as job responsibilities change.
- Viruses/Firewalls/Tampering Prevention (External). IT systems contains multilevel safeguards allowing system to both log and detect viruses, security violations, and tampering.
- Data Back-Ups and Recovery Plans. Company has a plan to prepare and recover from unforeseen incidents. Company conducts system back-ups daily that are stored in a safe that is fireproof and only accessible to IT Manager and senior executives. Additional back-ups are stored off-site weekly with a bonded company.
- Hardware Security. System server is stored in a fireproof locked room where access is restricted and tracked.
- Accountability. A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. Violators must be subject to disciplinary actions.

MAGUSA LOGISTICS

Best Practices - Further Details
Key Areas/Processes

MAGUSA
LOGISTICS

Business Partner Requirement

- Service Provider Requirements (Best Practice):
  - Exclusive Representative
    - An exclusive account representative at the foreign service provider is assigned to the company's account.
  - Prohibiting Subcontracting
    - Include clause in service contract prohibiting subcontracted services.
  - Requiring Background Clearances
    - Service providers must conduct comprehensive criminal background investigation on contract employees.
    - Service providers must submit bio-data with pictures and copies of background investigation.
  - Contractual Obligations
    - Incorporate obligation to security measures into service contracts. Includes:
      - Conducting an inspection of all empty containers/trailers prior to loading and documenting inspections,
      - Establishing seal control, issuance, affixing, and verification policies with appropriate checks and balances,
      - Tracking driver movements throughout transport,
      - Establishing access controls to the Company's cargo
      - Screening the employees who handle their cargo.
  - Establishing Procedures for Selection of Providers
    - Extensive written standards specify requirements for provider selection process.
      - Verification of provider's security measures
      - Financial solvency
      - Business references

MAGUSA LOGISTICS

Business Partner Requirement

- Customer Screening (Best Practice):
  - Preventing Misuse of Products by Customers.
  - Pre-screening Customers prior to engaging in business.
    - Verify validity of customer information, business references, run credit and business reports.
  - Keep current Customer information
  - Managing an Unknown Customer
  - Requiring Customer Registration
    - Requiring customers to register as “Known Consignors”, whereby must sign a declaration (with specific security measures) that has legal implications.
  - Using External Resources to Screen Customers
  - Requiring Business Referral
  - Meeting with Customers In-Person
    - Verify security measures: product packaging, staging, container/trailer inspections, and seal control.
  - Requiring Customers to Inspect Containers
  - Refusing Pick-Ups from Unknown Locations
  - Sending Representatives to Meet with New Foreign Customers
    - Verification of physical location, customers’ security, and reviewing references and conducting financial checks.

- Customer Outreach
  - Send to Customers letter to encourage them to enroll in the C-TPAT program and describing the minimum security requirements that customers are expected to meet.

MAGUSA LOGISTICS

Security Training and Threat Awareness (Best Practice - I)

- Awareness.
  - Initial and Periodic Training
  - Using Alert Levels
  - Communicating Terrorism Information to Employees
  - Multimedia training. Videos, Online Security courses, Intranet and Company Magazine. All training is documented by department supervisors, and periodically reviewed to ensure all employees have been trained.
  - Continuing Education. Keep abreast of latest cargo security procedures and technology.
- Specialized Training
  - Training in Areas of Specialty. Each employee trained in their areas of specialty.
  - Product Tampering, Collusion, Loss Prevention, Handling Breaches.
  - Conducting Background Investigations.
  - Segregating and Reporting Suspicious Containers.
  - Conducting 14-Point Trailer and Conveyance Inspections.
  - Highway Watch.
  - Utilizing External Resources
  - Security Guards

MAGUSA LOGISTICS

Security Training and Threat Awareness (Best Practice - II)

- Outreach
  - Collaborating with Local Law Enforcement
  - Training Business Partners
  - Translating Training into Multiple Languages
  - Receiving Updates From Association
- Employee Incentives.
  - Providing Incentives to employees for reporting security anomalies and recommending ways to improve the Company's security.
- Incident Reporting
  - Establishing a Hotline. A 24/7 anonymous "hotline" that is available to all employees and vendors (globally) to report suspicious or criminal conduct within the organization, as well as questionable business ethics.
  - Outsourcing Hotline. There are posters displayed throughout the facility and handouts regarding reporting procedures are distributed to employees.
  - Issuing Emergency Contact Information. Including CBT FAST Office, and the CBP hotline 1-800-BE-ALERT
  - Issuing Business Integrity Cards to all associates worldwide. Card provides contact information and instructions for employees to discreetly report suspicious activities and violations to corporate security staff and terrorists threats to CBP via 1-800-BE-ALERT.

MAGUSA LOGISTICS