APEC Private Sector

Supply Chain Security Guidelines

Contents

Executive Summary

- Key elements of supply chain security include:
  - Physical Security
  - Access Control
  - Personnel Security
  - Education and Training Awareness
  - Procedural Security
  - Documentation Processing Security
  - Trading Partner Security
  - Conveyance Security
  - Crisis Management and Disaster Recovery
- Elements of supply chain security pertain differently to each organization.
- Focus on elements of greatest importance to your organization.
- Complex, multi-country supply chains demand more collaboration on security issues.
- Security inside the organization is not sufficient. Collaboration outside the organization is essential.
- Conduct security assessments and implement security plans. Update regularly.
- Comply with international standards and requirements set by the World Customs Organization, the International Maritime Organization, the International Standards Organization, etc.

Physical Security

Physical security includes security measures that monitor and control the facility's exterior and interior perimeters. This will include Mail Service Security, Lock and Key Control, and Perimeter and Interior Alarms.

Recommended features, to be installed as appropriate:

- Appropriate peripheral and perimeter barriers.
- Electronic security systems, to include theft alarm systems, access control systems, closed circuit television (CCTV).
- Clear identification of restricted areas.
- Locking devices on external and internal doors, windows, gates and fences. Exterior doors and windows should be equipped with alarms.
- Segregated and marked domestic, international, high value, and dangerous goods cargo areas within the warehouse, preferably by a safe, caged or otherwise fenced-in area.
- Emergency lighting / power systems for key operational areas and high value cargo areas.
- Periodic inspection and repair to assure integrity of security measures.

Recommended procedures, to be conducted as appropriate:

- Depending upon its size, the company may require a security organization.
- Gates or doors through which vehicles or personnel enter or exit should be manned or under observation by management or security personnel.
- Access to employee parking should be controlled.
- Employee parking separate from visitor parking.
- Private passenger vehicles should be prohibited from parking in cargo areas or immediately adjacent to cargo storage buildings.
- Lock and key control, including signing in and out of high-risk areas.
- Restrict access to document or cargo storage areas.

Access Control

Access controls prohibit unauthorized access to facilities, conveyances, vessels, aircraft, shipping, loading docks, and cargo areas. If access control is not possible, increased precautions in other security aspects may be needed.

Recommended procedures, to be conducted as appropriate:

- Use of access control points and the positive identification, recording, and tracking of all employees, contractors, visitors, and vendors.
- Access control system for persons and vehicles.
- Procedure to challenge unauthorized / unidentified persons.
- Deny access and trigger an alarm when visitors attempt to enter an unauthorized area.
- Inspect vehicles required to access operations areas.
- Control the times individuals have access to facilities.
- Post a map of restricted areas within the view of employees and visitors.

Personnel Security

Personnel security is concerned with the screening of employees and prospective employees, as appropriate and as allowed for by law.

Recommended procedures, to be conducted as appropriate:

- Review skill requirements for key positions.
- Verify job application information.
- Check background of employees in sensitive positions.
- Contact references.
- Investigate criminal records, if any.
- Assure correct alignment of job skill requirements with individual's skills.
- Conduct periodic background checks, note unusual changes in social and economic situation.
- Check background and corporate structure of independent contractors.
- Implement drug consciousness programs.
- Drug testing (as allowed for by law):
  - Before hiring
  - Random periodic testing
  - At times of reasonable suspicion
- Employee identification (ID) procedures.
- ID cards or bracelets.
- Different color ID cards to designate access privileges.
- Different color uniforms for each sensitive area.
- Different color uniforms for security staff.
- Gate passes should be issued to truckers and other onward carriers to control and identify those authorized to enter the facility.

Education, Training and Awareness

Education, training and awareness encompass education and training of personnel regarding security policies, encouraging alertness for deviations from those policies and knowing what actions to take in response to security lapses.

Recommended procedures, to be conducted as appropriate:

- Communicate security policies and standards to employees, including consequences of noncompliance.
- Participation of all personnel in security awareness and training programs.
- Recognition for active employee participation in security controls.
- Incentives for individuals or employees reporting suspicious activities.
- Use press releases, email distribution lists and bulletin boards.

Procedural Security

Procedural security assures recorded and verifiable location of goods in the supply chain. Procedures should provide for the security of goods throughout the supply chain. Contingency procedures should be included within the scope of procedural security.

Recommended procedures, to be conducted as appropriate:

- Record and verify introduction of goods into the supply chain under the supervision of a designated security officer.
- Record and verify removal of goods from the supply chain under the supervision of a designated security officer.
- Protect against unmanifested material being introduced into the supply chain.
- Properly store empty and full containers to prevent unauthorized access, including the use of tamper-proof/non-counterfeitable seals.
- Check empty container received for storage or loading to assure its structure has not been modified.
- Establish procedure for affixing, recording, tracking, and verifying tamper-proof/non-counterfeitable seals on containers, trailers, and railcars.
- Seals should not be used in strict numeric sequence nor should seals be registered and controlled by a single person.
- Verify the identity and authority of the carrier requesting delivery of cargo prior to cargo release.
- Procedure for detecting shortages, overages, irregularity or illegal activities.
- Procedure for notifying Customs and other law enforcement agencies of suspected illegal activities.
- Proper marking, weighing, counting and documenting of cargo/cargo equipment, verified against manifest documents
- Procedure for tracking the timely movement of incoming and outgoing goods.
- Random, unannounced security assessments.
- Inspection of persons and packages.
- Additional security procedures for high-value and high-risk goods.

Documentation Processing Security

Documentation processing security, both electronic and manual, assures that information is legible and protected against the loss of data or introduction of erroneous information.

Recommended procedures, to be conducted as appropriate:

- Safeguard computer access and information.
- Control access to information systems, both by level of job responsibility and level of information sensitivity.
- Physical security in computer areas.
- Monitor employee use of data systems.
- Processes to backup computer system data.
- Record the amount of cargo by packing unit type, packing conditions, and security seal stamps. Discrepancies should be recorded with a note, photograph and scale weight records.
- Signatures required for all process checkpoints (e.g., document preparation, when seals are applied/broken, truck inspection, opening the vault, cargo delivery, cargo receipt, counting unshipped pieces, etc.)
- Fix times for the preparation of documents, and for the shipping and unshipping of cargoes.
- Use special control procedures to prepare emergency/last-minute shipments and if necessary notify authorities regarding such shipments.
- Software system should register transactions or support operations and, if possible, make a follow up of the activities that it handles.
- Record the entrance and exit time of people receiving and delivering goods.
- Document significant process delays.
- Ensure manifests are complete, legible, accurate, and submitted in a timely manner.

Future automated data exchange-related procedures

- Establish electronic customs reporting systems based on World Customs Organization Customs Data Model and the Unique Consignment Reference.
- Establish advance manifest reporting systems.

Trading Partner Security

Trading partner security extends supply chain security to your suppliers and customers. Communication, assessment, training, and improvement are key components.

Recommended procedures, to be conducted as appropriate:

- Encourage trading partners/suppliers/contractors to assess and enhance, if required, their supply chain security.
- Request written security agreements with trading partners/suppliers/contractors to include controls such as:
    - Tamper-proof/non-counterfeitable seals
    - Signatures
    - Time controls
    - Agreed means of communication
- Consider offering incentives to trading partners/suppliers/contractors for enhanced security coordination and cooperation.
- Document mutual supply chain security policies.
- Extensive exchange of information between trading partners/suppliers/contractors.
- Advise Customs and foreign authorities of security agreements with trading partners.
- Education, training and awareness by trading partners on supply chain security.
- If possible, include equivalent security provisions as a condition of contract for contractors/suppliers providing services.

Conveyance Security

Conveyance security provides protection against the introduction of unauthorized personnel and material into the supply chain, including the areas between the links of the supply chain.

Recommended proc edures, to be conducted as appropriate:

- Routinely search all readily accessible parking, storage, loading and transit areas.
- Secure internal/external compartments and panels.
- Procedures for reporting instances in which unauthorized personnel, unmanifested materials, or signs of tampering of a conveyance are discovered.
- When high-value or high-risk cargo must be transported a substantial distance from the point of unloading to a special security area, vehicles capable of being locked or otherwise secured should be used.
- Use locks, tamper-proof/non-counterfeitable seals or electronic seals to secure conveyances.
- If cost-effective, use transponders to facilitate continual tracking of conveyances.
- Use automatic electronic transmittal of 'smart card' data to Customs if available.
- Use 'smart card' technology containing vehicle, consignment, and driver information where automated border crossings are in place.
- Consider cost and future standardization issues related to use of smart cards, electronic seals and transponders.
- Stay informed regarding development of standards and requirements regarding smart cards, electronic seals and transponders by World Customs Organization, International Maritime Organization, International Standards Organization, etc.

Crisis Management and Disaster Recovery

Crisis management and disaster recovery procedures include advance planning and process establishment to operate in extraordinary circumstances.

Recommended procedures, to be conducted as appropriate:

- Emergency Plan
    - Crisis Management Team (CMT)
    - Emergency Response personnel in-house
    - Periodic updates and walk-through

- Crisis Management Rooms
    - Primary and alternate off-site locations

- Training
    - Periodic
    - Emergency Response personnel - ongoing

- Testing
    - Emergency Plan

- Compliance Reporting
    - Senior Location Leadership Certification - all locations

- Incident tracking and information coordination
- Investigation capability and follow-up
- Law enforcement role and linkage
- Analysis of cause of crisis

References

- **Business Anti-Smuggling Coalition (BASC) Security Program**

- **Customs-Trade Partnership Against Terrorism (C-TPAT) Guidelines**

- **World Customs Organization (WCO) Supply Chain Security and Facilitation**
    - **Advance Cargo Information Guidelines**

- **IBM Corporate Security Guidelines**