

Supply Chain Security Guidelines

September 12, 2003

**Patrice Knight
Vice President, Import Compliance Office
International Business Machines Corporation
Route 100
Somers, New York 10589
914-766-2318
e-mail: knighp@us.ibm.com**

Contents

Executive Summary	3
Industry / Trade	5
Governments	6
Port Authorities / Terminal Operators	8
Risk Analysis	9
Physical Security	10
Access Control	12
Personnel Security	13
Education and Training Awareness	14
Procedural Security	15
Documentation Processing Security	16
Information Security	17
Incident Management/Investigations	18
Trading Partner Security	19
Conveyance Security	20
Crisis Management and Disaster Recovery	21
References	22

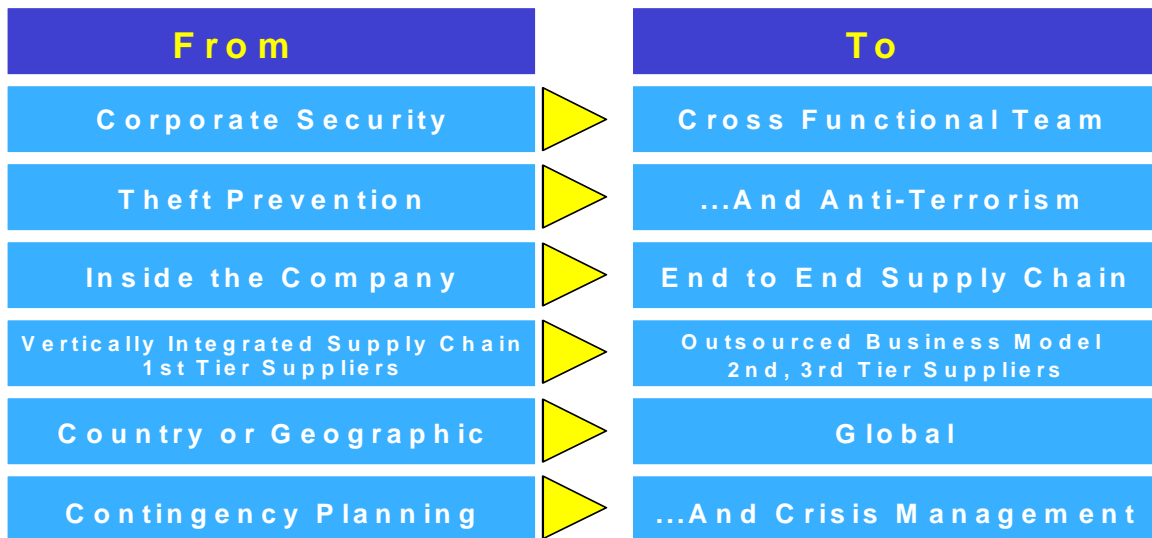
Notice

This paper presents a summary of supply chain security guidelines published by numerous sources (see References). It does not constitute legal advice regarding supply chain security or any specific matter.

Executive Summary

Supply Chain Evolution

Supply chains are evolving in many respects:



Supply Chain Security Stakeholders

- Trade / Industry
- Governments
- Port Authorities / Terminal Operators

Supply Chain Security Elements

Key elements of supply chain security include:

- Risk Analysis
- Physical Security
- Access Control
- Personnel Security
- Education and Training Awareness
- Procedural Security
- Information Security
- Incident Reporting and Investigations

- Documentation Processing Security
- Trading Partner Security
- Conveyance Security
- Crisis Management and Disaster Recovery

Supply Chain Security Considerations

- Many elements of supply chain security pertain to all organizations, but to differing degrees
- Focus on elements of greatest importance to your organization
- Complex, multi-country, and multi-vendor supply chains demand more collaboration on security issues
- Collaboration outside the four (4) walls of the organization is key to success

Industry / Trade

Industry, in collaboration with other companies, governments, government agencies, standards organizations, port authorities, industry, key trading partners, and other entities, are responsible for establishing and implementing supply chain security to assure the safety of people, country, and commerce.

- Enlist executive support
- Provide or utilize a standardized, consistent framework for evaluating security risk
- Document security policies / guidelines to include the following key elements:
 - Security education and training awareness
 - In-house security
 - Warehouse security
 - Transportation service provider security
 - Manifest security
 - Access control
 - Personnel Security
 - Information security
 - Document Processing Security
 - Risk Analysis
 - Physical Security
 - Procedural Security
 - Incident Reporting and Investigations
 - Trading Partner Security
 - Crisis Management and Disaster Recovery
- Build on existing systems and practices
- Perform periodic reviews of existing security measures
- Prioritize and address security deficiencies identified by periodic reviews
- Conduct regular security inspections to ensure the continuation and effectiveness of appropriate security measures
- Prioritize implementation based on risk management and the needs of your organization
- Establish a code of ethics and conduct to be followed by all executives and employees
- Conduct training, drills, and exercises to ensure familiarity with security plans and procedures

Governments

Governments, in collaboration with other governments, government agencies, standards organizations, port authorities, industry, key trading partners, and other entities, are responsible for establishing or endorsing security guidelines to assure the safety of people, country, and commerce, and for establishing or endorsing the means by which supply chain security representations may be validated.

- Provide or utilize a standardized, consistent framework for evaluating security risk.
- Prioritize implementation based on risk management
- Approve a Port Facility Security Plan and subsequent amendments
- Approve a Port Facility Security Assessment and subsequent amendments
- Test the effectiveness of the Ship or the Port Facility Security Plans, as appropriate
- Determine the port facilities required to designate a Port Facility Security Officer
- Exercise control and compliance measures
- Establish the requirements for a Declaration of Security
- Set security levels
- Ensure the provision of security level information to:
 - ships entitled to fly their flag
 - port facilities within their territory, and
 - ships prior to entering a port or whilst in a port within their territory
- Update security level information as circumstances dictate
- Establish procedures to verify that there is a valid International Ship Security Certificate or a valid Interim International Ships Security Certificate
- Establish written security agreements with other governments, government agencies, standards organizations, port authorities, industry, and key trading partners
- Incorporate aviation security standards into national civil aviation security programs
- Allow for the provision of alternative measures in small airports or ports
- Adopt a civil aviation quality control program to assure the effectiveness of the established national aviation security program
- Establish a security standards/program training program
- Use a common methodology to monitor/audit compliance
- Conduct inspections and investigations as necessary to assure security
- Perform unannounced inspections/assessments
- Prioritize security deficiencies identified by assessments

- Require written action plans to remedy identified deficiencies
- Develop a mechanism to determine if incoming flights from foreign country airports meet the essential security requirements
- Establish or endorse the means to validate supply chain security representations
- Perform or participate in incident management and contingency planning

Port Authorities / Terminal Operators

Port authority and terminal operator security is designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility. Many standard supply chain security elements pertain to port authorities and terminal operators. Additional security guidelines pertinent to port authorities and terminal operators are listed below.

- Establish and maintain the Port Facility Security Plan
- Prepare written and verifiable security procedures for areas under port/terminal control
- Conduct or participate in the Port Facility Security Assessment
- Respond to security level information issued by the Government
- Conduct physical searches of all readily accessible areas, as required
- Comply with applicable security guidelines and regulations
- Post conspicuous signs that describe established security measures
- Gather and assess information with respect to security threats and exchange such information with appropriate stakeholders
- Establish and maintain communication protocols for facilities and vessels
- Deter or prevent the introduction of unauthorized weapons, incendiary devices, or explosives
- Provide the means for raising the alarm in reaction to security threats or security incidents
- Conduct training, drills, and exercises to ensure familiarity with security plans and procedures
- Conduct regular security inspections to ensure the continuation of appropriate security measures
- Perform or participate in port security incident management and contingency planning

Risk Analysis

Risk analysis provides the foundation and justification for implementation of appropriate security measures.

The evaluation should include review of many elements including crime rates, value of assets, effectiveness of law enforcement and the criminal justice system in the locale where you are operating, past incident activity, and the potential for natural/man-made disasters.

With a risk evaluation completed, a comprehensive supply chain security program can be designed and implemented. Risk analyses should be periodically reviewed and updated to address business/environmental changes.

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.

- Buildings should be constructed of materials that resist unlawful entry and protect against outside intrusion
- Periodic inspection and repair to assure integrity of security measures
- 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.
- Perimeter fencing that encloses the yard and entire center where a cargo is held of sufficient height to impede entrance and exit.
- Gates or doors through which vehicles or personnel enter or exit should be manned or under observation by management or security personnel.
- Trash must be removed under a controlled process from sites/areas using visual inspection, metal detection, or X-Ray checking. Ensure that trash bins/containers are empty when put into service
- Optimal peripheral and perimeter barriers
- Segregated and marking of international, domestic, high value, and dangerous goods cargo within the warehouse by a safe, vault, caged or otherwise fenced-in area.
- Break areas and locker/change rooms must not be located inside storage or marshalling areas
- Lighting on the perimeter of a facility to illuminate loading/unloading areas and provide light or CCTV images.
- For shared facilities, there shall be lighting around the warehouse, trailers that contain cargo, offices, and points of entrance and exit, but not necessarily the total perimeter and yard of the facility;
- Depending upon its size, the company should have a security organization
- Emergency lighting / power systems for key operational areas and high value cargo areas
- Access to employee parking should be controlled by a gate/pass and/or decal system
- 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.
- Signing in and out of high-risk areas
- Restrict access to document or cargo storage areas
- Electronic Security Systems, to include theft alarm systems, access control systems, motion detectors, and closed circuit television (CCTV)
- Recorded CCTV coverage of loaded trailers, with recordings to be maintained for a specified period.

Access Control

Access controls prohibit unauthorized access to facilities, conveyances, vessels, aircraft, shipping, loading docks, and cargo areas.

- Use of access control points and the positive identification/verification, recording, and tracking of all employees, contractors, visitors, and vendors for 24 hours per day, 7 days per week.
- Access control system for persons and vehicles
- Procedure to challenge unauthorized / unidentified persons
- Access limitations on high value security areas and other restricted areas.
- 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
- Use metal detectors, if required
- Access authorization must be immediately removed or changed for any person who is terminated, separated or transferred. When a personal identification code is compromised, access authorization code must be immediately changed or deleted.
- Keys used to access storage areas must have a management accountability process: Daily accountability controls for keys in use by multi-persons for storage access. Keys must be logged in and out at a central control point. This control point must be in an enclosed facility with limited access.
- Search policy must be in place where legally permitted
- Airport identification cards and vehicle passes shall be checked at all airside and security restricted area checkpoints
- Establish a common definition of the critical parts of security restricted areas
- Screen all staff, including flight crew, together with items carried, before being allowed access into a security restricted area. If this is not practicable, persons and items shall be subjected to continuous appropriate random screening at a frequency indicated by risk assessments
- Conduct aircraft security searches and aircraft security checks after all service providers (e.g., caterers, cleaners, etc.) have left the aircraft
- Gate passes should be issued to truckmen and other onward carriers to control and identify those authorized to enter the facility
- Keep screened passengers of commercial flights separate from occupants of general aviation



Personnel Security

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

- Periodic background checks, including social and economic situation and new friends.
- Background and corporate structure of independent contractors
- Application verifications - separation of duties
- Personal investigations of the employees
- Investigations of criminal acts
- Investigation of references
- Drug consciousness programs
- Drug testing (as allowed for by law)
- Before hiring
- Random periodic testing
- At times of reasonable suspicion
- Identification (ID)/verification procedures
- ID cards or bracelets
- Different color ID cards to designate access privileges
- Different color ID cards to distinguish between employees, visitors, vendors, etc.
- Different color uniforms for each sensitive area
- Different color uniforms for security staff
- Review skill requirements for key positions
- Assure correct alignment of job skill requirements with individual's skills

Education and Training Awareness

Education and training awareness encompasses educating and training of personnel to the security policies, awareness of deviations from those policies and knowing what action to take.

- Participation in security awareness and training programs for all personnel
- Communicate security policies and standards to  employees, including consequences of noncompliance
- Detection and addressing unauthorized access
- Incentives for those individuals or employees reporting suspicious activities
- Recognition for active employee participation in security controls
- Maintaining cargo integrity
- Use of press releases and bulletin boards
- Managers and instructors involved in and responsible for security training of security and airport ground staff shall undergo  annual recurrent training in security and latest security developments
- Flight crew and airport ground staff training shall be conducted on an initial and recurrent basis for all airport and air carrier flight and airport ground staff
- Security staff shall be trained to undertake the duties to which they will be assigned (e.g., screening technology and techniques, screening check point operations, security systems and access control, baggage and cargo security, aircraft security and searches, weapons and restricted items, etc.)

Procedural Security

Procedural security assures recorded and verifiable introduction and removal of goods into 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.

- Verify the identity and authority of the carrier requesting delivery of cargo prior to cargo release.
- Recorded and verifiable introduction and removal of goods into the supply chain under the supervision of a designated security officer.
- Proper storage of empty and full containers to prevent unauthorized access, including the use of seals. For example, empty and full containers must remain locked and inside a secured fenced area until such time that they are backed up to a dock to be unloaded;
- Procedure for affixing, replacing, recording, tracking, and verifying seals on boxes, containers, trailers, and railcars.
- Procedure for affixing, replacing, recording, tracking, and verifying serialized tape 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
- Proper, secure storage of seals
- Procedures for detecting and notifying Customs and other law enforcement agencies of shortages and overages or anomalies and 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.
- Protection against unmanifested material being introduced into the supply chain.
- Inspection of persons and packages.
- Check empty container received for storage or loading to assure its structure has not been modified.
- Additional security procedures for high value goods.
- Written and verifiable security procedures

Documentation Processing Security

Documentation processing security assures that information is legible and protected against the exchange, loss, or introduction of erroneous information.

- 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.
- Printed names and signatures required for all process checkpoints and any suspicious process activities (e.g., document preparation, when seals are applied/broken, truck inspection, opening the vault, cargo delivery, cargo receipt, counting unshipped pieces, etc.)
- Fixed times for the preparation of documents, and for the shipping and unshipping of cargoes when they arrive.
- Special control procedures to prepare emergency / last minute shipments and notify the authorities regarding such shipments.
- Software system should register the transactions or support operations and make a follow up of the activities that it handles.
- Record the entrance and exit time of people receiving and delivering goods.
- Information is legible and protected against the exchange, loss or introduction of erroneous information
- Document significant process delays.
- Ensure manifests are complete, legible, accurate, and submitted in a timely manner.
- Establishment of advance manifest procedures.
- Participate in automated manifested systems where available

Information Security

Information security assures that information is protected against the exchange, loss, or introduction of erroneous information.

- Limit access to supply chain information to those with a “need to know”.
- Safeguard computer access and information.
- Control access to information systems.
- Physical security in computer areas.
- Processes to backup computer system data.
- Software system should register the transactions or support operations and make a follow up of the activities that it handles

Incident Management/Investigations

Incident management and investigations assures appropriate tracking and information coordination capability within an organization.

- A process is to be implemented for the timely reporting of lost and missing assets as well anomalies in the packaging/shipping process.
- Investigations should be initiated in a timely manner.
- Enablement / tracking
- Law enforcement role and linkage
- Root cause analysis should be a required element of every investigation to understand process deficiencies and protect against reoccurrence.

Trading Partner Security

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

- Request trading partners to assess and enhance, if required, their supply chain security
- Written security agreements with trading partners to include preventive controls such as:
 - Use of seals
 - Signatures
 - Time controls
 - Agreed to means of communication
- Documented supply chain security policies
- Employee policy manual
- Extensive exchange of information between trading partners
- Advise Customs and foreign authorities of security agreements with trading partners
- Education and Training Awareness by trading partners on supply chain security
- Review or establish contractual supply chain security obligations
- Where appropriate, include equivalent security provisions as a condition of contract for contractors / suppliers providing services
- Obligation: commitment, legislation, regulations, contract, risk, reward
- Suppliers of air carrier catering stores and supplies and air carrier cleaning services, stores, and supplies shall implement security controls to prevent the introduction of prohibited articles into such stores and supplies intended to be carried on-board aircraft.
- If the suppliers of air carrier catering stores and supplies and air carrier cleaning services, stores, and supplies are located outside the airport, all supplies shall be transported to the aircraft in locked or sealed vehicles
- Work with trading partners to identify, prioritize, and address supply chain security deficiencies

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.

- Physical search of all readily accessible 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 cargo must be transported a substantial distance from the point of unloading to the special security area, vehicles capable of being locked or otherwise secured must be used
- Use of locks, seals or electronic seals to secure conveyances
- Use of transponders to facilitate continual tracking of conveyances
- Automatic electronic transmittal of 'smart card' information to Customs
- Automate border crossings by use of a 'smart card' that contains vehicle, consignment, and driver information
- Prior to entering a port or while in a port, comply with the requirements for the security level set by that Government, if such security level is higher than the security level set by the Administration for that ship
- Identify and use only secure stops during transport
- Communication link with the driver(s) – radio, cell phones or equivalent – must be in place
- For 'high risk' shipments provide
 - Two drivers
 - Global Positioning System (GPS) tracking of vehicle and load
 - Escorted service if necessary
 - Driver security training
 - Vary routing
 - Pre-advise and tracking from point-to-point
- Conduct aircraft security searches and aircraft security checks after all service providers (e.g., caterers, cleaners, etc.) have left the aircraft
- Screening equipment shall provide for the necessary detection to ensure that prohibited articles are not carried on board conveyances
- Screening systems shall provide automatic threat recognition to facilitate the operator's search

Crisis Management and Disaster Recovery

Crisis management and disaster recovery procedures include advance planning and establishing processes to prepare, coordinate, and operate in extraordinary circumstances.

- Emergency Plan that includes:
 - Crisis Management Team (CMT)
 - Emergency Response personnel
 - Periodic updates and scenario testing
- Training
 - Periodic
 - Emergency Response personnel - ongoing
- Testing
 - Emergency Plan



References

- **Business Anti-Smuggling Coalition (BASC) Security Program**
- **Customs-Trade Partnership Against Terrorism (C-TPAT) Guidelines**
- **European Parliament and the Council of the European Union**
- **Common Rules in the Field of Civil Aviation Security**
- **International Business Machines (IBM) Corporate Standards and Security Guidelines**
- **International Maritime Organization (IMO)**
- **Technology Asset Protection Association (TAPA) Freight Security Requirements (FSR)**
- **United States Coast Guard**
- **World Customs Organization (WCO) Supply Chain Security and Facilitation**
- **World Customs Organization (WCO) Advance Cargo Information Guidelines**