EMERSON

Supplier Supply Chain Security Requirements

Since the 9/11 attacks in the United States, the U.S. developed the Customs Trade Partnership Against Terrorism ("CTPAT") program to address border security and supply chain risks. After that the World Customs Organization ("WCO") adapted the SAFE framework of standards to secure and facilitate global trade, which became the basic concept of Authorized Economic Operator ("AEO"). Many countries have implemented voluntary government-industry supply chain security ("SCS") partnership programs. These initiatives are meant to strengthen overall supply chain and border security around the world.

Under these supply chain security programs, the governing agencies expect businesses to ensure the integrity of their international shipments/supply chain and actively communicate and enforce their security guidelines to their non-domestic business partners within the supply chain. In return, many agencies offer benefits such as fewer examinations, quicker and more reliable clearances, eligibility for periodic duty payments and allowance for self-policing.

While not required, Emerson recommends that all suppliers become members/partners in their region's supply chain security program. Regardless of formal participation in a regional program, all Emerson suppliers shipping internationally are ***required*** to establish and implement supply chain security controls (as outlined in this document) to ensure the integrity of their international shipments and facility security controls in accordance with the Emerson Electric requirements.

Supply Chain Risk Assessment

Security Vision & Responsibility

Emerson suppliers should have company controls in place that highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband.

Business Partner Security

Emerson suppliers must exercise due diligence to ensure their business partners meet the supply chain security criteria outlined in this document. Emerson suppliers must understand their business partners' commitment to supply chain security. The business partner commitment can be required through contract language, annual communication, and/or purchase order terms and conditions.

Physical/Facility Access Controls

Emerson suppliers should have access-control devices that enable them to control who has access to their building(s) as well as a personnel identification system in place for positive identification and access control purposes. Access to sensitive areas should be restricted based on job description or assigned duties. Visitor access must be monitored and controlled, including drivers delivering or receiving cargo. The supplier should have processes in place to positively identify drivers before cargo is received or released. Additionally, Emerson suppliers are expected to have procedures in place to identify, challenge, and address unauthorized/unidentified persons. When an employee leaves or is terminated from the company, Emerson suppliers must have controls in place to remove access to buildings, networks and devices.

Physical Security

Physical security of Emerson supplier locations is a critical part of supply chain security. Emerson supplier facilities must be constructed of materials that resist unlawful entry, such as steel, brick or concrete. Regular inspections by guards and periodic evaluations by facilities managers are to be used in maintaining the integrity of structures. Building problems that compromise security are to be immediately reported by employees and repaired. Emerson suppliers are expected to have secure locking devices installed on interior and exterior windows and doors to prevent the unlawful entry of persons in accordance to any local fire escape regulations. When not in use, gates within and outside of the facility must be secured with locking devices.

Each facility must have adequate lighting at entrances, exits, fence lines, building exterior, cargo handling areas and parking areas. Gates where vehicles and/or personnel enter or exit (as well as other points of egress) should be manned and/or monitored. Lighting should be kept in good repair and part of every facility inspection. Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances. When warranted by risk, perimeter fencing should enclose the areas around cargo handling and storage facilities.

Emerson suppliers should consider the use of security technology (Cameras, security systems, badge readers, etc.) and should have written policies/procedures governing the use, maintenance and protection of the technology.

Personnel Security

As local country laws permit, supplication information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law. Employees should not be affiliated with known terrorist groups or organizations with strong political opinions and/or actions against any specific country or region.

Procedural Security Controls

Emerson suppliers must have procedures in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time. When cargo is staged overnight, or for an extended period, measures must be taken to secure the cargo from unauthorized access. Cargo staging areas, and the immediate surrounding areas, must be inspected on a regular basis to ensure these areas remain free of visible pest contamination.

Container/Conveyance and Seal Security

When applicable, the physical integrity of Container/Conveyances must be verified prior to unloading and/or loading. Container/Conveyances must be stored in a secure area to prevent unauthorized access. Containers/Trailers/Cargo Units used for Emerson shipments must be equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container’s locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.

Emerson suppliers must have written controls and current training programs/materials to ensure employees in the shipping and receiving departments understand and perform the appropriate inspection processes prior to unloading and/or loading Container/Conveyances. Inspections of conveyances must be systematic and must be conducted at conveyance storage yards. Where feasible, inspections must be conducted upon entering and departing the storage yards and at the point of loading/stuffing.

All full container shipments that can be sealed must be secured immediately after loading/stuffing/packing by the responsible party (i.e. the shipper or packer acting on the shipper’s behalf) with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals.

Emerson suppliers’ seal verification process must be followed to ensure all high security seals (bolt/cable) have been affixed properly to Containers/Trailers/Cargo Units and are operating as designed. The procedure is known as the VVTT process:

> V – View seal and container locking mechanisms; ensure they are OK;
> V – Verify seal number against shipment documents for accuracy;
> T – Tug on seal to make sure it is affixed properly;
> T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.

Agricultural Security

Emerson suppliers must have written procedures designed to prevent pest contamination. Containers/Conveyances and the freight/cargo staging areas must be inspected on a regular basis to prevent pest contamination of international freight. The appropriate measures must be taken if pests are found within the facility and/or located near cargo. Indicators of Pest Activity or Contamination identified during inspections include:

- Insects or Insect eggs
- Pest nests (birds, bees, etc.)
- Snails or Slugs
- Any type of soil (contaminants can be within soil)

- Plant debris and/or Seeds

If contaminants or pest activity is identified during an inspection, immediate action is required. Methods of treatment could include, but are limited to:

- Pesticide usage – if the identified pest is unknown, a pest control professional must be contacted immediately
- If the contamination/pest is found in wood packaging materials, the wood can be retreated according to the ISPM 15 standards.
- Clean the area where the pest/contamination was identified.

These procedures must include compliance with Wood Packaging Materials (WPM) regulations, as applicable. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).

Education, Training and Awareness

Emerson suppliers must establish, provide and maintain a security training and awareness program for its employees, vendors and partners to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers.

Cybersecurity Controls

To defend Information Technology (IT) systems against common cybersecurity threats, Emerson suppliers must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in all computer systems used in its business. Suppliers must ensure that their security software is current and receives regular and timely security updates in accordance with industry standards.