OGUK

Security of Supplies and Materials Guidance for Shipping Cargo and Materials Throughout the Supply Chain

Guidelines

Issue 1
September 2021

Background

The Security of Supplies and Materials Task Finish Group was convened in January 2019 to address security concerns from Operators and service providers who had identified gaps in the industry regarding the movement of cargo via freight transport from suppliers to bases and onto offshore facilities. The main aim of this group was to deter, detect, delay, and deny any unauthorised materials or people. To achieve this aim, the Task Finish Group has developed this industry guidance document for shipping cargo and materials throughout the supply chain. This has been made possible by sharing good practices from logistics, security and cyber security practitioners.

This guidance document does not supersede any other applicable Standards and is designed to complement them wherever possible and is applicable to all stakeholders in the supply chain.

Security Plans, Emergency Procedures and Business Continuity Plans, audits and verification arrangements should be put in place and drills and exercises conducted regularly to ensure they remain effective.

Implementing these guidelines will improve your overall resilience, reduce the number of business disruptions you suffer and the damage they cause. In addition, these guidelines can be used by your suppliers in the development and security management of their own processes, products and services.

Acknowledgments

In preparing and publishing this document, Oil & Gas UK would like to recognise the significant contribution that has been made by the following organisations whose shared knowledge and expertise has been invaluable in the development of this Guidance Document.

- ASCO Group Ltd.
- Peterson UK Ltd.
- CNOOC
- TAQA
- Apache
- Neptune
- Equinor
- INEOS

ISBN: 1 903 004 73 2
PUBLISHED BY OIL & GAS UK

London Office:

1st Floor, Paternoster House, 65 St Paul's Churchyard, London, EC4M 8AB
Tel: 020 7802 2400 Fax: 020 7802 2401

Aberdeen Office:

4th Floor, Annan House, 33-35 Palmerston Road, Aberdeen, AB11 5QP
Tel: 01224 577250 Fax: 01224 577251

info@oguk.org.uk

www.oguk.org.uk

September 2021

Contents

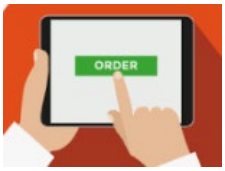
Introduction

The whole Supply Chain process for the North Sea oil and gas Industry has been analysed and documented into 12 separate processes. This document has taken every section of the process and provided a description of the process, the security threats for the process and the recommended controls that should be put in place to ensure that the threats are managed.

Cyber security threats and the required controls are covered in Section 12 and should be considered alongside every other stage of the process.

This document can be used as a whole, or each process can be reviewed individually depending on your interest in the process.

The 12 sections are outlined in the table below:

	**Security when Ordering Goods** • Contracts • Production of service/goods request • Creation of Purchase Order • Agreed Supplier List
	**Security During Load Preparation (Vendor / Supplier)** • Delivery of goods/materials to Warehouse/factory • Selection of goods/materials • Preparation of Delivery Note
	**Security during the Picking and Packing of Materials** • Selection of goods/materials • Preparation of goods/materials • Packing goods/materials • Storage of goods/materials in CCU • Sealing of CCUs with Anti-tampering Unique Number Tags

	**Security during Ground Transportation** • Loading of CCUs/Goods onto transportation vehicles • Moving transportation vehicle • Resting transportation vehicle • Delivery of CCUs/Goods
	**Security at Supply Base/Goods Receipt Point** • Delivery of CCUs/Goods • Delivery of unannounced goods/packets • Storage of CCUs • Storage of unannounced goods/packets • Handling Dangerous Goods/firearms
	**Security when Packing for Offshore** • Wrapping goods/materials • Storage of packages in CCUs
	**Security when Marshalling Cargo** • Moving CCUs around the yard
	**Security when Manifesting** • Preparing a Manifest List • Adding Anti-tampering Unique Number Tags to Manifest

	**Security during Loading to Vessel** • Loading of CCUs to Vessel • Secure CCUs
	**Security during Sea Transportation** • Safe and Secure Transportation of Cargo at sea
	**Security when Offloading to the Installation** • Sabotage • Manifest tampering • Activists and protest groups
	**Cyber Security** • Using applications and online platforms to place purchase order • Receiving invoices via email • Systems for labelling goods and tracking them

1. Security when Ordering Goods

The sourcing of goods or services is the first step within the Supply Chain process and is not an activity undertaken in isolation. This section will provide awareness of the Security risks and control measures to be considered when negotiating and collaborating with vendors at the start of the Supply Chain process.

Within businesses, procurement has become a cross functional activity involving many people and many suppliers. Procurement practitioners should be aware of the potential risks of the release of sensitive information and fraudulent attempts which can cause financial and reputational damage to their companies.

Entering relationships with vendors for sourcing products or services can expose the company to security threats such as fraud, theft, bribery and blackmail. Risks to and from the supply chain can take many forms. For example, a supplier may fail to adequately secure their systems, they may have a malicious insider or supplier's personnel may fail to properly handle or manage information. Understanding these risks is key to ensuring security measures and mitigations are proportionate, effective and responsive.

In order to prevent and mitigate such security risks, we can apply specific tools and policies to reduce the likelihood of an incident occurring during the early stages of the supply chain ordering process.

1.1 Security Threats

The potential security threats that are possible during the goods ordering process are listed below:

Fraud - wrongful or criminal deception intended to result in financial or personal gain by means of ordering goods for personal use or financial gain by a supplier.

Examples

- Purchase orders being issued to friends or family members.
- Inferior quality or standards of goods being ordered to meet budget restrictions.

Insider Threat - a malicious threat to a company that comes from people within the company, such as employees, former employees, contractors or business associates, who have insider information concerning the organisation's security practices, data and computer systems.

Examples

- Ordering goods for a malicious intent.
- Employee user accounts are compromised.
- Ordering goods from unsecure/fake webpages.

Contraband - goods that have been imported or exported illegally.

Examples

- Orders from online vendors that are delivered directly to shore base (drugs, alcohol, cigarettes, inappropriate materials).

Bribery - buyers are dishonestly persuaded to act in a supplier's favour by accepting gifts or money or other inducements.

Examples

- Buyers receive gifts or financial gain to award contracts to a specific supplier who provided the gifts.
- Buyers' friends/family receive financial gain.

Extortion/Blackmail - an individual or an organisation obtains something, usually money, through force or threats.

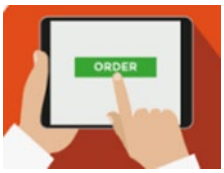
Examples

- Employees are coerced into changing bank details of suppliers.
- Extorting commercially sensitive information.
- Computer gets infected after receiving a phishing email that results in a demand for payment to restore the system.

1.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the ordering process.

- Demonstrate good governance with clear security responsibility and accountability within the organisation, up to and including senior management/board level.
- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.
- There should be evidence and use of risk management policies, processes and procedures to manage security risks.
- Control the number of individuals who are authorised to purchase goods.
- Identification of security information and handling of sensitive information within the supply chain process.
- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.



- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting and investigating any security incident.
- Explain the security risks to your suppliers. Promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.
- Segregation of duty where more than one individual is involved in the ordering process. This will reduce the risk of individuals being able to order and goods receipt an item without any further checks being done.
- A financial authority matrix should be in place so that it reduces the risk of large sums being approved throughout the company.
- An approved vendor list is established to purchase goods/services from reliable sources.
- Well documented ordering processes and ensure these processes can be measured and audited.
- Train all buyers in the Order process to ensure they understand and follow the process.
- Develop and issue a company Code of Business Conduct, e.g., a set of principles designed to guide workers to conduct themselves with honesty and integrity in all actions representing the company.
- Business Continuity Plans (BCP) to ensure that there is a backup plan should the ordering process fail. The BCP should contain a process on how to continue ordering safety critical items and services.

2 Security During Load Preparation (Vendor/ Supplier)

When goods have been ordered they are then prepared for transportation by road, sea and/or air to an offshore installation. The load preparation that takes place at the vendor's or supplier's premises provides opportunities for individuals or groups to compromise security.

All vendors and suppliers need to be selected through a robust, approved supplier process and their ability to ensure the security of the goods they prepare for loading, independently verified. The integrity of any goods or packages can be compromised by malicious individuals or groups who are intent on causing harm, criminal acts or disruption.

The selection and verification of vendors/suppliers should identify and test all the potential security threats and the control measures that have been put in place to ensure that the integrity of their security is robust. Where this cannot be demonstrated, it is imperative that corrective actions are agreed between the purchaser and the vendor/supplier to rectify this and provide the necessary assurance.

In addition to having a robust security management system for load preparation, the supplier approval process should also focus on the vetting of employees and the provision of adequate supervision.

2.1 Security Threats

The potential security threats that are possible during the load preparation at the vendor's or supplier's premises are listed below.

Sourcing and procuring vendors/suppliers - engaging the services of or purchasing goods from non-approved suppliers.

Examples

- The selection and approval of a vendor/supplier is based predominantly on cost and inadequate consideration of security.
- Demand for a certain product or service being deemed as urgent or an emergency and decisions are taken to use a non-approved supplier.
- Familiarity with vendors/suppliers over prolonged use.

Insider Threat - failing to effectively vet supplier/vendor employees.

Examples

- Insider threat because personnel have not been effectively vetted through the recruitment and selection procedures.
- Inadequate levels of supervision are in place to ensure that load preparation activities are delivered in accordance with the requirements of company procedures.

Procedural Inadequacies - written instructions that omit key security requirements.

Examples

- Insufficient consideration is given to security during load preparation.
- Failing to apply security procedures effectively.
- Easily defeated checklists being utilised.
- Failing to actively monitor (audit and verify) procedures to confirm their suitability to prevent security breaches.
- Dispatching freight / cargo without informing the recipient.

The consequences of these threats being realised can vary significantly with the worst case being a terrorist activity designed to disrupt and gain maximum media exposure. These usually involve loss of life and damage to infrastructure.

2.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the ordering process.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.
- There should be evidence and use of risk management policies, processes and procedures to manage security risks.
- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.
- Explain security risks to your suppliers, promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.
- A robust company procedure and system for identifying and selecting approved suppliers and vendors who have the capability to provide high standards of security.
- Robust and well applied auditing and verification arrangements for approved suppliers and vendors.
- Effective control over the use of "one off" suppliers/vendors should be in place.
- Effective control over access to completed load lists.
- Clear and robust procedures/standards for load preparation by suppliers and vendors.
- Specific attention and controls when required to individual items when required such as tamper proof seals and control of custody for medical supplies, delivered directly into a warehouse for onward transportation.

- Train company warehouse personnel on goods receipt and Load Preparation procedures to ensure they understand and follow it.

3 Security During the Picking/Packing of Materials

The Packing of Goods received from Vendors/Suppliers for shipment to offshore installations should be considered a potential security risk.

The risks are predominately around theft, sabotage or smuggling of goods destined for offshore installations.

Companies who undertake the picking and packing of goods should be approved through the Achilles FPAL (First Point Assessment Limited) registration scheme and subject to audit verification. Their process should have robust controls to counteract these risks.

Employees involved in the process should be subject to vetting, which should include background checks. Personnel should be trained and competent in the prescribed process, which should include security control measures including the physical examination of goods. Additional control measures such as sniffer dogs and X-Ray machines may also be considered.

The area in which the Picking/Packing and sealing of containers is undertaken should have restricted access. Prior to closing and sealing Cargo Carrying Units (CCU's), they should be subject to final security checks. On completion of these checks, the CCU should be sealed using pre-numbered, tamper proof seals. All documentation pertinent to the loading and shipping of the CCU's should refer to the seal number to enable cross-checks to be made to ensure that the validity of the sealing process is maintained throughout the process.

3.1 Security Threats

The potential security threats that are possible during the picking and packing of goods received from Vendors/Suppliers for shipment to offshore installations are listed below.

Procedural Inadequacies - missing and inadequate for the task.

Examples

- Insufficient consideration is given to security.
- Failing to apply security procedures effectively e.g., control of dangerous goods.
- Failing to actively monitor procedures, audits, and verification.
- The absence of a recorded procedure for the physical checking of cargo and containers prior to their shipment to the Supply Base.

Fraud - wrongful or criminal activities intended to result in financial or personal gain.

Examples

- Theft of goods for personal gain.
- Knowingly under issuing stock.

Inadequate Physical Security - where risk assessment has failed to identify the necessary physical security measures, or they have been identified but not installed.

Examples

- Controlled access points.
- Physical barriers.
- CCTV

Insider Threat - failing to effectively vet supplier/vendor employees.

Examples

- Lack of vetting process for the personnel responsible for picking/packing cargo who may have malicious intent.
- Disgruntled employees in a role where they can cause disruption to the activities.
- Sabotage of site assets/cargo/packages
- Potential for smuggling of contraband to offshore installations
- Inadequate control of materials that leaves the potential for theft

3.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the picking / packing of materials.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.

- There should be evidence and use of risk management policies, processes and procedures to manage security risks.

- Identification of security information and handling of sensitive information in the Supply Chain process.

- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.

- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting and investigating any security incident.

- Explain security risks to your suppliers, promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.

- Use of approved vendors responsible for packing, checking and sealing CCU's to ensure that unauthorised materials are not shipped out to offshore installations and that theft, sabotage and vandalism of material does not occur.

- Employees should be trained and competent with relevant picking and packing standards to ensure their understanding by following the applicable security measures.
- Secure access control in place for picking, packing and storage of loaded CCUs
- Cargo security checks to ensure that the correct cargo is loaded as per the authorised load list prior to the CCU being sealed on both open and closed CCUs through physical inspection and use of sniffer dogs.
- Facilities to X-Ray any suspect materials prior to packaging.
- Use of uniquely numbered CCU door seals with the number being identified on the manifest.
- The completion of relevant manifests identifying CCU contents, Dangerous Goods, and signed confirmation that security checks have been undertaken by approved personnel.

4 Security During Land Transport

Transportation of goods by road should be considered a potential security risk, in that journeys can be both short and/or long in their duration and that a requirement could exist for goods to be left unattended during transit e.g., driver breaks and refuelling stops.

The risks are predominantly theft, although sabotage and smuggling of goods offshore should also be considered and should be controlled through the security risk assessment.

Transport companies/hauliers should be in possession of the correct licences/permits, e.g., an Operator's Licence. Within the offshore industry, special attention should also be paid to the transportation of dangerous goods. The security requirements for the carriage of dangerous goods are split into two levels. There is a general level of requirements applicable to all dangerous goods (Classes 1-9) and additional provisions for high consequence dangerous goods (HCDGs).

Companies should have a process for handling both non-hazardous goods and hazardous goods. This process should include the vetting of drivers, security training, and dangerous goods training, if dangerous goods are being transported.

The process should also include a Transport Security Plan (a legal requirement for dangerous goods transportation) which should identify all physical barriers, control systems and controlled access measures. It is also imperative regular exercises are conducted, confirming the suitability of emergency response arrangements.

The Department of Transport has produced a guidance document (Security Guidance on the Carriage of Dangerous Goods by Road and Rail) to help organisations such as carriers and consignors with the secure transport of dangerous goods. This includes helping small or new enterprises with limited security experience to implement security measures applicable to their transport operation and help demonstrate that any relevant or mandatory security requirements of Chapter 1.10 of the ADR and RID Regulations are being met.

4.1 Security Threats

The potential security threats that are possible during land transport are listed below:

Theft - the wilful removal of goods from both open and closed CCU's intended for offshore operations.

Examples

- Theft of essential goods in order to disrupt operations.
- Theft of expensive items destined for offshore.
- Theft of precious metals, either destined for offshore or backloaded, that can be scrapped for cash.

Sabotage - CCU's or material for offshore is sabotaged by driver or driver allows sabotage to occur.

Examples

- Sabotage to CCU's or lifting gear on CCU's to cause disruption.
- Sabotage to materials located in open or closed CCU's.

Smuggling - driver smuggles items into CCU or allows items to be smuggled into CCUs

Examples

- The driver smuggles or allows the smuggling of contraband into a CCU.
- The driver smuggles or allows the smuggling of suspicious packages, offensive weapons that could be used in an attack offshore.

Insider Threat - a malicious threat to a company that comes from the driver who has insider information concerning the organisation's security practices.

Examples

- Enabling components to build a bomb or suspicious packages to be loaded into a CUU whilst being transported.
- Enabling offensive weapons to be loaded into a CCU which could be used in an attack.
- Drivers receive bribes in return for allowing a breach of security.

4.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the transportation of goods overground.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.

- There should be evidence and use of risk management policies, processes and procedures to manage security risks.

- Identification of security information and handling of sensitive information within the supply chain process.

- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.

- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting and investigating any security incident.

- Explain security risks to your suppliers, promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.

- Transport companies should have relevant processes and procedures to ensure valid driving licences, and ADR checks are carried out.
- Transport companies should be able to demonstrate compliance with all legal obligations, in relation to ensuring vehicles, trucks, vans, and trailers are road worthy and are tested/inspected for the goods they are carrying.
- Transport companies should be aware of the need for a goods vehicle operator licence to carry goods in a lorry, van or other vehicle with either:
    - a gross plated weight (the maximum weight that the vehicle can have at any one time) of over 3,500 kilograms (kg)
    - an unladen weight of more than 1,525 kg (where there is no plated weight)
- Transport companies should be encouraged to have live vehicle tracking and productivity with real-time visibility of vehicle location and route analytics and make use of Journey Management Planning where feasible.
- Transport companies are encouraged to have fit recordable front and rear facing cameras to capture security breaches, and ensure the cameras remain functional.
- Any closed CCU loaded onto trailers should be secured using a unique numbered container door seal.
- Where radioactive material, firearms and/or ammunition are being transported in closed CCUs, these should be secured using an approved British Standard padlock.
- Parked vehicles with trailers carrying CCUs should not be left unattended. This is best achieved by using a second person or by parking in a staffed secure parking area monitored by security personnel.
- An approved transport security plan should be in place for all transport companies transporting dangerous goods. This should be supported by emergency response and business continuity plans.
- Access and egress to transport parking areas for cargo should be staffed, with CCTV, fences and locked gates to prevent unauthorised access.
- The keys and spare keys for vehicles should always be controlled and always known.

5 Security at a Supply Base/ Goods Receipt Point

The Supply Base/Goods Receipt Point is open to potential exploitation which may manifest itself in the delivery of suspect goods/packages or malicious individuals with the intent to cause harm, criminal acts, or disruption through active protest.

All Supply Base/ Goods Receipt Points should have a robust process to mitigate these risks. The process should identify the person(s) responsible for security who should audit the process to ensure that it is robust and is being applied and maintained 24/7.

The process should include a site security plan which should identify all physical barriers, control systems, and controlled access measures.

This process should also include the vetting of employees, training, and the duties to be undertaken to maintain secure access and egress on site. These duties should include (but not be limited to) the stop and search of personnel and vehicles and the inspection of containers/packages. The inspection may be limited to physical examination but could also include more robust measures including sniffer dogs and X-Ray machines.

The security plan should also refer to the site Emergency Response Procedure which in turn should include additional security measures to be taken to increase site security if the threat level changes.

5.1 Security Threats

The potential security threats that are possible when goods arrive and are being processed at any supply base goods receipt point are listed below.

Unannounced Goods - packages that were not expected by the recipient and have been delivered unexpectedly.

Examples

- Personal items trying to be shipped outside of the company's procedures.
- Purchases from online suppliers being addressed to the supply base.
- Goods that have been organised by the company, but they have failed to inform the supply base.
- Late or overdue goods that were cancelled by the company and find their way back into the delivery schedule.

Poor Cargo Handling Processes - employee actions that compromise security.

Examples

- Incompatible packaging.
- Goods being incorrectly processed and forwarded to the wrong installation.
- Accidental damage and sabotage of goods.

Inadequate Security Control Measures - a failure to properly assess the security risks and/or implement effective control measures.

Examples

- There is no requirement to sign in and produce photo identification.
- Poor or non-existent CCTV or alarms.
- Inadequate procedures for checking goods that have been delivered.
- Staff are unaware of security issues.

Unauthorised Visitors/Protestors - people who gain access to the goods receipts area without permission.

Examples

- Delivery drivers and their passengers.
- Employees from different operational departments are within the Supply Base.
- Protest group infiltration by imposters.

Terror Threat from Suspect Packages - unopened packages (closed box policy) and deliveries that are left unattended.

Examples

- The company specifies that the package cannot be opened at Goods Receipt.
- Goods dropped off by delivery drivers without gaining authorisation.

Access to Pyrotechnics (Flare Guns) - gaining unauthorised access to secure cabinets.

Examples

- Control of keys and access codes for secure cabinets.

Crime (Theft) - the wilful removal of goods intended for offshore operations.

Examples

- Theft of essential goods in order to disrupt operations.
- Theft of expensive goods for personal gain.

Weak Process around Control Areas - complacency of the staff in the goods receipt area.

Examples

- Leaving the counter unattended or access to the area open.
- Poor control of documentation.
- Accepting goods without the correct paperwork and checks.
- Being deliberately distracted to enable malicious intent.

5.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring at the Supply Base/Goods Receipt Point.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.
- There should be evidence and use of risk management policies, processes and procedures to manage security risks, including how to handle unannounced goods.
- Identification of security information and handling of sensitive information within the supply chain process.
- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.
- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting and investigating any security incident.
- Explain security risks to your suppliers, promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.
- Appoint a person responsible for security who coordinates this with others on the supply base.
- Effective goods receipt procedures that are regularly audited and verified as suitable and sufficient.
- Consider the introduction of Bar-Coding systems to clearly identify goods.
- Agreements with clients and their vendors for the random searching of containers and boxes.
- Physical controls to restrict unauthorised access to the goods receipt area. This should include secure card entry for access to all warehouse areas.
- Supply Base perimeter security arrangements that include:
    - Installation of industry standard security fences and gates.
    - Enough security guards to conduct patrols of the Supply Base perimeter.
    - Access control systems are integrated with CCTV, lighting, intrusion detection, locks and barriers that detect activity and delay access.
- Develop an appropriate access control system to stop, check and search personnel and vehicles.
- Procedures and physical control measures are in place for the safe storage and transportation of pyrotechnics, including flare guns.

- Ensure the doors and windows provide adequate levels of security for the goods receipt areas.
- When packing CCU's, ensure that the container has unique numbered door seals fitted before leaving the packing area. The unique number should be added to the manifest.

6 Security when Packing for Offshore

Packing for offshore involves the picking of materials, the packing of materials, the sealing of CCUs where applicable and the locating of materials/CCUs in a secure area, destined for offshore.

In order to prevent and mitigate risk, base operators should be accountable for providing controlled areas with physical control measures, where access is strictly controlled to avoid unauthorised personnel having access to materials/CCU's. Personnel working in a secure area should be subject to background checks. Written confirmation should be given of any visitors to unauthorised sites. Visitors should also be in possession of some form of identification.

Consideration should be given to both air and sea freight as both could pose the same threats. In addressing the threats, it is vital that a security plan/security risk assessment for the site is completed with roles and responsibilities for security described and undertaken. It is worth noting that bases located within harbours are also subject to the International Ship and Port Facility Security (ISPS) Code.

Sea freight will be packed in either open or closed containers. Closed containers will be sealed with a uniquely numbered tamper proof seal which is recorded on the manifest. There will be occasions where closed CCUs will be required to be padlocked for added security. This applies to CCUs containing radioactive materials, some types of arms and explosives, and sometimes valuable items. Open top containers should be scrutinised to ensure items are not placed in units after packing, as these units are impossible to secure, but at all times they should remain in a secure area or staffed, when out with a secure area.

Procedures for hazardous goods should be in place covering all classes and it is imperative that the correct labelling and documentation, fully compliant with IMDG/ADR prior to shipment, is in place. Check/audits should be undertaken to verify compliance with legislation.

6.1 Security Threats

The potential security threats that are possible when goods are being packed for offshore are listed below.

Inadequate Security Control Measures - a failure to properly assess the security risks and/or implement effective control measures.

Examples

- There is no requirement to sign in and produce photo identification.
- Poor or non-existent CCTV and alarms.
- Employee identification and visitor passes are not in operation.
- Inadequate procedures for sealing containers and storing materials destined for offshore either by air or by sea transport.
- Staff are unaware of security issues.

Insider Threat - a malicious threat to a company that comes from people within the company, such as employees, former employees, contractors or business associates, who have insider information concerning the organisation's security practices, data and computer systems and the opportunity to pack items destined for offshore.

Examples

- Packing components to build an explosive device.
- Packing offensive weapons or objects to be used in an attack.
- Being bribed to pack items into a container.

Contraband - goods that have been imported or exported illegally.

Examples

- Ordered from online vendors and delivered direct to shore base (drugs, alcohol, cigarettes, inappropriate materials).

Terrorists - individuals or groups that are intent on causing disruption through high profile activities.

Examples

- Packaging of explosive devices in with the cargo that is destined for an offshore installation.
- Tampering with foods that are destined for the offshore installation with the intent of causing illness, death, and disruption to operations.
- Packaging of hoax devices designed to cause confusion and interrupt the operation of the installation.

Poor Packaging/Sabotage - the deliberate packing of cargo in such a way as to create disruption to the operation.

Examples

- The inability to unpack the cargo safely leading to delays and disruption of operations.
- Cargo is packed poorly in order to cause it to become damaged during transit or when it is being unpacked.
- The deliberate targeting of high value or critical process equipment.
- Sabotage at the picking/packing stage could go unnoticed as the packer is usually the person that closes the container door and applies the seal.

Unattended Cargo - cargo destined for offshore presents numerous threat opportunities, e.g., open top containers are less secure than closed containers and are a considerable risk to the industry.

Examples

- Open top containers placed close to a perimeter fence.
- Containers being packed are left open or unattended during staff breaks or fire drills.

6.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the packing for offshore process.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.
- There should be evidence and use of risk management policies, processes and procedures to manage security risks and for the control of Dangerous Goods.
- Identification of security information and handling of sensitive information within the supply chain process.
- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.
- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting any security incident.
- Explain security risks to your suppliers promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.
- Supply Base/Warehouse/yard perimeter security arrangements that include:
    - Installation of industry standard security fences and gates.
    - Enough security guards to conduct patrols of the Supply Base perimeter.
    - Access control systems are integrated with CCTV, lighting, intrusion detection, locks and barriers that detect activity and delay access.
- Robust and implemented procedures should be in place for the picking, packing, sealing and storage of containers. This should include the requirement for uniquely numbered tamper proof seals and the recording of the unique number.
- Robust background checks should be carried out on employees working in the picking/packing function and photo identification cards should be issued to all employees.
- Visitors should be in possession of some form of photo identification and should inform the site prior to the visit.
- Visitors should be issued with a visitor's identification card, which should be displayed at all times.
- Site security audits (both desk-top and physical security) should be regularly undertaken to check physical security and test the security plan/procedures.

- IMDG/ADR training is mandatory for those packing materials destined for offshore. It is recommended that this training is approved and regularly refreshed. Security awareness training should also be provided for employees to make them aware of the International Ship and Port Facility Security (ISPS) Code and the current threat level.

7 Security when Marshalling Cargo

Once materials/goods have passed the stringent Receipt/Shipment checks, they are containerised and marshalled in designated areas in preparation for shipment to offshore installations.

Once the containers are closed, there are generally no further checks done on the contents until the container reaches its offshore destination. Therefore, as this is the last line of defence, it is vital that the marshalling area has a robust security plan, and access to this area is restricted to authorised personnel only.

The area should be fenced off, or have visible segregation from other areas, with the appropriate level of signage denoting that the area is restricted access only and monitored by CCTV and security patrols. Signage should also show that security searches will be undertaken on personnel and cargo; these may be random or with cause.

Personnel working in a secure area should be subject to background checks. It should be made clear that anyone accessing the area without the correct level of clearance will be removed and may be the subject of further action.

All containers should be sealed with uniquely numbered tamper proof seals, which should be cross-referenced on the appropriate documentation and cross checks made at the appropriate points throughout the transportation and loading process.

Particular focus should be placed on the procedures/controls related to containers containing Hazardous Goods including, but not restricted to, explosives, radioactive materials, and firearms (Flare Guns and Cartridges).

Emergency Response exercises should be undertaken at regular intervals to test the robustness of these controls/procedures and to identify where improvements need to be made.

7.1 Security Threats

The potential security threats that are possible when goods are being marshalled within the supply base are listed below.

Unattended Cargo - open top containers / pipes placed in unsecure areas.

Examples

- Inadequate process for controlling access to marshalling yard.
- Opportunity to tamper with containers and insert materials designed to become dropped objects or cause disruption offshore.

Inadequate Supervision and Procedures - any failure to monitor the security of the marshalling activities within the supply base.

Examples

- Inadequate application of The International Ship and Port Facility Security Code.

- Supervision levels are insufficient to provide effective control over activities.

Insider Threat - a malicious threat to a company that comes from people within the company, such as employees or contractors.

Examples

- Packing offensive weapons or objects to be used in an attack.
- Being bribed or forced against their will to use their position to tamper with cargo.

7.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the marshalling of cargo.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.
- There should be evidence and use of risk management policies, processes and procedures to manage security risks including the secure marshalling of cargo and for the control of Dangerous Goods.
- Identification of security information and handling of sensitive information within the supply chain process.
- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.
- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting and investigating any security incident.
- Explain security risks to your suppliers, promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.
- Supply Base/yard perimeter security arrangements that include:
    - Installation of industry standard security fences and gates.
    - Enough security guards to conduct patrols of the Supply Base perimeter.
    - Access control systems that are integrated with CCTV, lighting, intrusion detection, locks and barriers that detect activity and delay access.
- Visitors should be in possession of some form of photo identification and should inform the site prior to the visit.
- Visitors should be issued with a visitor's identification card, which should be displayed at all times.

- Employees working within the supply base/yard will be issued with photo identification cards that should always be worn while working.
- Site security audits (both desktop and physical security) should be regularly undertaken to check physical security and test the security plan/procedures.
- IMDG training is mandatory for those marshalling CCUs containing hazardous goods for offshore. It is recommended that this training is approved and regularly refreshed. Security awareness training should also be provided with employees being made aware of the International Ship and Port Facility Security (ISPS) Code and the current threat level.

8 Security when Manifesting

A manifest is an itemized list of a ship's cargo, used to identify what goods are being transported offshore. The generation of a manifest and non-manifested cargo should be considered a potential security risk.

The risks are predominately around smuggling of goods destined for offshore installations either through non-manifested goods or incorrect manifesting of goods. Theft could also be a consideration should the manifest fall into the wrong hands and goods become attractive and potential targets for theft.

The person compiling manifests should be aware of the risks including falsely documented goods, goods not manifested, or goods not itemised correctly e.g., one lot. Employees and companies should also be aware of the risks of manifests falling into the wrong hands, or leaks of information, resulting in manifested goods being communicated to unauthorised employees/non-employees.

It is therefore imperative that all employees involved in the manifesting process should be subject to company vetting processes, which should include background security checks and references. Personnel should be trained and competent in the manifesting process and should be confident to intervene, address and correct discrepancies or errors made on manifests.

With emerging technologies, the threat of online security should also be considered a substantial risk with adequate control measures in place, around IT security, preventing cyber-attacks or loss of sensitive information.

8.1 Security Threats

The potential security threats that are possible when manifesting goods for shipping are listed below.

Insider Threat / Theft - a malicious threat to a company that comes from people within the company, such as employees and contractors colluding with people outside of the company to move stolen goods.

Examples

- Theft of goods for personal gain.
- Leaking of company information resulting in business disruption.
- Falsely documented items.
- Employee user accounts are compromised.

Contraband - goods that are being shipped illegally.

Examples

- Ordered from online vendors and delivered direct to shore base (drugs, alcohol, cigarettes, inappropriate materials).
- Goods are not manifested or manifested in insufficient detail.

8.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the manifesting for shipping process.

- Where possible limit the distribution of all sensitive information and utilise secure operating areas. This should include arrangements for the control of all visitors and site access/egress.
- Provide controlled access that guarantees the security of the facilities where goods and cargo are stored and handled.
- Conduct robust personnel security checks, e.g., background checks when recruiting and interviews for leaving or fired employees.
- Consider the use of numbered container door seals.
- Provide training and regularly measure the competence of the Manifester.
- Conduct site security audits, inspections, and spot checks.
- Where possible, use Bar Coding linked directly to the manifest.
- Contractual arrangements - use a sufficient business partner evaluation system for the selection of low risk and high security compliant suppliers, clients and subcontractors.
- Conduct random and with cause searches of people and containers.
- Retain the ability to change security levels based on the current threat levels within your region.
- Procedures for the control and segregation of Dangerous Goods within CCUs and on the supply vessels deck. These procedures should include controls for firearms.
- Onboard vessel checks for sensitive manifest information and its effective control.
- Conceal the identity of vessels that are potentially transporting cargo that could be considered a security target.

9 Security During Loading to the Vessel

The Supply Base is open to potential exploitation which may manifest itself in suspect goods/packages being put into containers by malicious individuals with the intent to cause harm, criminal acts, or disruption through active protest.

The Supply Base should have a robust process to mitigate these risks. ISPS standards (via Port Authority or nominee) should be in place. The standard should identify the person (s) responsible for security and is being applied and maintained 24/7.

This process should also include the vetting of employees, training, and the duties to be undertaken to maintain secure access and egress on site. These duties should include (but not be limited to) the stop and search of personnel and vehicles and the inspection of containers/packages. The inspection may be limited to physical examination but could also include more robust measures including sniffer dogs and X-Ray machines.

The security plan should also refer to the site Emergency Response Procedure, which in turn should include additional security measures to be taken to increase site security if the threat level changes.

9.1 Security Threats

The potential security threats that are possible while loading to a vessel are listed below.

Insider Threat - a malicious threat to a company that comes from people within the company, such as employees and contractors colluding with people outside of the company to move stolen goods.

Other Examples

- Theft of goods for personal gain.
- Opportunity to put packages into containers.
- Using another infrequently utilised port facility.
- Activist or protest group members.
- Vessels third party activities e.g., tank cleaners, marine surveyors, food deliveries, crew changes, waste skips or taxi services.
- Deliberate sabotage of cargo to create disruption or incidents.

9.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during the loading of the vessel.

- The adoption and promotion of a good security culture with a programme to maintain awareness, including running staff security awareness campaigns to ensure that the staff are security conscious.

- There should be evidence and use of risk management policies, processes and procedures to manage security risks including security when loading/unloading of vessels.

- Relevant measures should be applied to personnel security for individuals who work within the Supply Chain. This may include vetting, background checks, identification of security sensitive positions, Drug and Alcohol testing, and visitor management.
- Robust cargo checking arrangements in place when loading the vessel that include, but are not limited to:
    - Ensure the cargo identification numbers match the load list.
    - Arrangements for dealing with non-conforming cargo/incorrect identification numbers.
    - Ensure the correct destination labels are attached and the CCU test date does not have less than 30 days before mandatory re-certification is needed and that it is free from obvious damage.
    - Confirming that the unit type and size corresponds with the load list and that the Hazards Placards are in place.
    - Check for any damage to the lifting gear and for potential dropped objects.
    - Check that the doors are closed and secured by an accepted and recognised method e.g., safety seal, padlock or ty-wrap.
    - Check the contents of all open containers.
- Protocols are in place for managing security incidents, including 'near-misses', and the arrangements for reporting and investigating all security related incidents.
- Supply Base perimeter security arrangements that include:
    - Installation of industry standard security fences and gates.
    - Enough security guards to conduct patrols of the Supply Base perimeter.
    - Access control systems that are integrated with CCTV, lighting, intrusion detection, locks and barriers that detect activity and delay access.
    - Random checks using sniffer dogs.
- Issue employees working within the supply base/yard with photo identification cards that should always be worn while working.
- All visitors should be in possession of some form of photo identification and should inform the site and have gained approval prior to their visit.
- Site security audits (both desktop and physical security) are regularly undertaken to check physical security and test the security plan/procedures/Business Continuity Plans.
- IMDG training is mandatory for those marshalling CCUs containing hazardous goods for offshore. It is recommended that this training is approved and regularly refreshed. Security awareness training should also be provided with employees being made aware of the International Ship and Port Facility Security (ISPS) Code and the current threat level.

- Training and procedures should be in place for the control of Dangerous Goods as hazardous goods in numerous forms will be loaded and stored in accordance with control of the Dangerous Goods Act.
- Apply the ISPS Standards (via Port Authority or nominee) including:
    - Badge controls
    - Procedures – authority for shipping
    - Emergency response procedures (Fire / Bomb threat)
    - Site security audits
- Random searches of people and containers
- Control of Dangerous Goods – Dangerous Goods and firearms should only arrive at the quayside when the boat is set to sail. The position of class 1 & 7 goods on the vessel will be taken into consideration.
- Quayside staff to provide a copy of the Load list and any Dangerous Goods Lists to the vessel's representative for the installation that they are visiting.

10 Security During Sea Transportation

Supply chain vessels are vulnerable to physical and cyber security incidents stemming from various threat factors and the supply chain that supports them, both when in operational use and when undergoing maintenance or refit.

The main security concern is the smuggling of illegal contraband destined for offshore installations. However, there are underlying risks regarding activism, terrorism, crime, disgruntled personnel, stowaways, and cyber-attacks.

Drones present an important developing threat as they can easily circumvent security measures around port perimeters, severely compromising security.

A comprehensive legislative framework underpinned by the International Ship and Port Security (ISPS) Code exists to protect companies from the consequences of unlawful intentional acts against shipping and port operations.

The ISPS code is a mandatory instrument for all countries party to the International Maritime Organisation (IMO's) International Convention for the Safety of Life at Sea (SOLAS). It guarantees that ships and port facilities are implementing minimum international standards of maritime security.

However, gaps still remain in its implementation and companies responsible for vessels should be aware of current security risks and consider the threats and control measures mentioned in this document.

10.1 Security Threats

The potential security threats that are possible during shipping to and from an offshore installation are listed below.

Insider Threat - a malicious threat to a company that comes from people outside of the company, such as crew members, contractors or activists acting on their own or as part of a wider protest group.

Examples

- Crew members paid or forced to put packages into containers for terrorist attacks.
- Activist or protest group members who deliberately sabotage cargo to create disruption or incidents.

Protestors/Activists - organised groups who try to block the vessel's passage/access to the installation or board the vessel without consent.

Examples

- Protestors or activists on the sea.
- Stowaways getting onboard vessels with the intent of causing damage or disruption to operations.

10.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of incidents occurring during the sea transportation process.

- Specified security requirements within the contractual arrangements between the supply vessel owners and the hirer.
- Relevant measures should be applied for personnel security for individuals who work onboard the Supply Vessels, including vetting and background checks.
- Shipping companies should have conducted a security risk assessment and implemented all the necessary control measures to protect the ship and its systems. These control measures are to be employed to protect the vessel from threats in order to deter, detect, delay, and deny unauthorised access to the ship.
- Exercises and drills should be carried out to ensure familiarity with the security procedures aboard the ship.

Additional Control Measures that are to be considered (In line with the ISPS code 3 levels)

Level - 1	Level - 2	Level - 3
- Access control of all personnel and equipment to vessels, including CCTV, lighting, barriers and photographic ID cards - Monitor restricted areas - All vessels' security duties are adhered to as per the ISPS code and ship security plan - Monitoring deck areas and areas surrounding the vessel - Supervision of cargo handling and stores - Ensure security communication is available - Ensure liaison with the port facility to ensure a designated secure area for inspection and searching.	- Assigning additional personnel to patrol decks during silent hours - Limit the number of access points to the vessel, identify those to be closed and a means of securing them - Deter waterside access in liaison with the port and base facility - Establish a restricted area on the shoreside in cooperation with the port and base facility - Increase the frequency and detail of searches of people's, personal effects and cargo - Escort visitors on the vessel - Provide additional specific security briefings to all vessel personnel on any identified threats, emphasising the need to report suspicious people, objects or activities and stressing the need for increased vigilance - Carry out a full or partial search of the vessel.	- Limit access to a single controlled access point - Grant access only to those responding to a security incident or threat thereof - Suspension of embarkation or disembarkation - Suspension of cargo handling operations and deliveries - Evacuation of the vessel - Movement of the vessel - Preparing for a full or partial search of the vessel

11 Security when Offloading to Installation

In the event of a vessel offshore becoming subject to protest action, the OGUK Guidance document - "Oil and Gas - Response to Protest Actions 2019" gives recommendations on how to respond and details of how the crew of the asset might deal with situations that arise.

The response to any type of threat / protest should be based on the acceptance that protesters have a right to peaceful protest. There is, however, a limit as to what protesters can do in pursuance of their cause before some activities contravene criminal or civil law.

When a vessel begins to offload onto an installation, this is the last stage in the transit of the cargo where it can remain open to a security threat and at risk from someone who is intent on causing damage or disruption.

11.1 Security Threats

The potential security threats that are possible during the offloading of cargo to an installation are listed below.

Insider Threat - the inadequate vetting of vessel crew members.

Examples

- Opportunity to put packages into containers for terrorist attacks.
- Activist or protest group members who deliberately sabotage cargo to create disruption or incidents.

Protestors/Activists - creating obstacles to disrupt offshore operations

Examples

- Blockade of the installation.
- Unauthorised occupation of the installation.

Procedural Breaches - a failure to comply with 500 metre zone restrictions.

Examples

- Failing to obtain entry permission to the safety zone from the control room.
- Manoeuvring the vessel without authority.

11.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring while offloading to an installation.

- Security plan for the offloading of goods and checking manifest against the CCU contents

- Providing training and ensuring competence in the correct handling of Dangerous Goods that are being delivered to the platform
- Have a protestor action plan to respond to and manage any potential incident. The plan should be tested through drills and exercises with all the necessary stakeholders
- Consider delaying or re-routing transportation of supply vessels during incidents
- There should be evidence and use of risk management policies, processes and procedures to manage security risks
- There should be protocols for managing security incidents, including 'near-misses', and arrangements for reporting and investigating any security incident.
- The adoption and promotion of a good security culture with a programme to maintain awareness including staff security awareness campaigns being run to ensure that the staff are security conscious
- Explain security risks to your suppliers, promote and adopt the sharing of security information across your supply chain to enable better understanding and anticipation of emerging security attacks.

12 Cyber Security

The supply chain is large and complex, and technology can be used to facilitate this chain from the early stages of evaluating products and ordering goods to offloading them to the installation. It is also an essential element of communications, tracking goods and transferring them securely offshore.

Using applications and online platforms to place purchase orders, receiving invoices via email, labelling goods and tracking them, putting in CCTV to monitor restricted areas, controlling access to secure places and many more, all rely on ever-growing technology which exposes the industry to a wide range of cyber security risks.

Nowadays, internet connections carry communication between organisations and suppliers, which makes the supply chain even more complicated. This also reduces the visibility of our vulnerabilities and significantly exposes us to cyber risks. Since inherited vulnerabilities are not visible to us, they can easily be exploited at any point in the supply chain. This could be anything from a weakness in technology, misconfiguration of software, human mistakes, or intentional misuse.

Therefore, essential cyber security controls are needed throughout the supply chain in order to mitigate these risks to an acceptable level.

12.1 Security Threats

The potential security threats that are possible from a cyber-attack are listed below.

Vulnerable Vendor/supplier - any vendor with poor security posture can cause damage and disruption as a chain is as strong as the weakest link.

Examples

- Theft of goods for personal gain.

Social engineering, phishing emails, Vishing, Smishing - the use of deception to manipulate individuals into divulging confidential information over the phone, via email, voice mail or SMS.

Examples

- Sending a well-crafted invoice via email to deceive an individual into clicking on a link or opening an attachment.

Business Email Compromise (BEC) - a cybercrime where a hacker compromises a vendor user account and sends a well-crafted email from a compromised account over to the targeted organization.

Examples

- The customer receives an invoice from their vendor's trusted contact with attachments or a link to an invoice. This is very hard to detect and is almost always successful.

Malware, Spyware, Ransomware or Polymorphic viruses - any software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system can interrupt services and communication in the supply chain.

Examples

- Ransomware encrypts and blocks access to information that at least damages the vendor's reputation.

Online fraud or scam - a type of deception which makes use of the Internet and could involve hiding information or providing incorrect information for the purpose of tricking victims out of money.

Examples

- The procurer purchases goods from a fake website instead of legitimate websites and makes payment.

Collusion - secret cooperation in order to deceive others.

Examples

- Secret cooperation to issue labels to send illegal goods offshore.

Cyber Espionage /Data Leakage/Exfiltration/Manipulation - unauthorised access to read information or to manipulate it.

Examples

- Criminals gain unauthorised access to CCTV recorded videos.

Service Disruption / Denial of Service Attack - any unavailability of services such as CCTV, communications, or purchase order system.

Examples

- Blocking access to CCTV to cover unauthorised entrance to secure areas or interrupting communications.

Insider Threat - disgruntled individuals or human mistakes, and even compromised privileged accounts can cause damage.

Examples

- Removing information about an illegal parcel on the system is an intentional insider threat and leaving the default admin password of the access control system can be an unintentional insider threat.

Natural/Manmade Disasters - these events can cause significant damage to computer system.

Examples

- Flood or lightning surges can cause damage to electronic devices which have a security impact. Safety systems such as automated fire suppression or automatic dial up alarm systems can be manipulated by insiders or remote hackers and cause severe damage.

12.2 Control Measures to be Considered

To prevent the threats listed above, the following controls should be considered to reduce the likelihood of an incident occurring during manifesting for the shipping process.

- Consider adopting Cyber Essential controls to protect your organization and encourage your suppliers to get certified.
- Conduct a cyber risk assessment prior to approving a vendor/supplier to understand what their security looks like. Follow the NCSC guidance.
- Choose suppliers from the government approved list, verify supplier on the NCSC website.
- Add the right to audit in your contracts to ensure the visibility of continuous improvement of their security controls/posture.
- Raise awareness within your suppliers and build a trust relationship to share cyber intelligence and communicate incidents to contain them or learn lessons from each other's incidents.
- Raise awareness within your staff to improve the security culture within your company, empower them against social engineering attacks and encourage them to report any suspicious activities to the security incident response team.
- Enrol focused training program for staff based on their role's risk level.
- Develop a Security Incident Response plan and make sure the team understands their roles and responsibilities and conduct tests to ensure preparedness. Use the "Exercise in a Box" tool, which is an online tool on the NCSC website to help organizations find out how resilient they are to cyber-attacks and practise their response in a safe environment.
- Consider security in the early stage of every IT network, hardware or software design, development and implementation of security controls including but not limited to CCTV, building management systems, UPS, and access control systems.
- Implement technical security controls such as firewall, Anti-Virus, host-based IDS/IPS, Application whitelisting, Multi-factor authentication, secure remote access.
- Avoid enabling unnecessary services and access rights.
- Proactively identify vulnerabilities and fix them using workarounds or patch management.
- Closely monitor privileged user accounts including IT admins and enable auditing and logging for accountability.

- Use banners on computer systems for raising awareness and use it as a deterrent control.
- Define and enforce security policies, such as password policies. and use technology to enforce them.
- Define standards and an acceptable use policy.
- Avoid using free tools and applications for sensitive communications and security services. Set protocols and implement pre-defined rules if you should use them.
- Conduct background checks and have staff sign an NDA prior to employment.
- Enforce mandatory vacation longer than 2 weeks and Separation & segregation of duties to detect fraud. Job rotation detects collusion during employment.
- Enforce the termination policy to remove all access to IT systems immediately before termination. All IT devices should be returned immediately.
- Categorise labels and classify assets into defined categories and implement suitable access control accordingly. IT assets include data, devices and services, licences and people.
- Define a clear hardware life cycle and data retention and disposal policy. Consider data privacy laws such as GDPR and other relevant legislation. Follow the ICO guidelines.
- Build your data centre in different geographic risk regions or on the cloud to reduce the risk of natural/manmade disasters.
- Keep a copy of your critical data offsite in a safe place, physically disconnected from the network. That would be your last hope post-ransom attack.

Appendices

A Audit Checklist

To assist all the stakeholders that have a part to play in ensuring the security of supplies and materials being shipped to offshore installations, the following checklist can be utilised to audit your existing arrangements.

Reviewer's Name	
Audit Date	
Tel. Number	
Email Address	
Company	

Overview

Serial	Subject
1.	Personnel security
2.	Physical security
3.	Storage and distribution
4.	Shipping information control
5.	Information Security
6.	Records and documentation
7.	Facility photos
8.	Corrective action plan

The suppliers, supply base companies and operators have a collective responsibility to ensure Supply Chain Security Standards and will be assessed by security audits. Corrective action plans will be completed timely and correctly.

Facility Profile and Structure

1.	Facility name		
2.	Facility address/postcode		
3.	GPS location		
4.	Contact person's name		
5.	Tel. number		
6.	Email/website		
7.	Total number of workers	Permanent:	Temporary:
8.	Key products		
9.	Number of buildings: Administration Workshops Warehouses Container yards Laydown yards Others		

Part 1 – Personnel Security

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
1.1	Is there a procedure in place to screen prospective employees and to periodically check current employees? A process for hiring & interviewing applicants?				
1.2	Application information, such as employment history and references, must be verified prior to employment.				
1.3	Does the supplier / company keep each employee's ID copy and personal file?				
1.4	Background checks and investigations should be conducted into prospective employees.				
1.5	Periodic checks and reinvestigations for existing employees should be performed based on cause and/or the sensitivity of the employee's position.				
1.6	Is there a procedure in place to monitor the handover of badges, keys/cards, tools, and authority of system login-in when the employee resigns? Check the records.				
1.7	Do the security staff adequately control the issuance and removal of employees, visitor and vendor ID badges? Does the security dept have a list of all personnel authorised to work every day?				
1.8	Do all employees receive basic security awareness training, including new employee orientation and periodic refreshers for existing employees?				
1.9	Do security personnel receive training in maintaining cargo integrity, identifying internal conspiracies, and protecting access control?				
1.10	Personnel must be made aware of the procedures the company has in place to address emergencies and how to report it (e.g., a hotline).				
1.11	Are personnel encouraged to report irregularities, suspicious activities and/or security violations? If yes, please indicate by which means?				
1.12	Are documented security procedures publicised throughout the facility?				

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
1.13	Is a threat awareness program established and maintained by management to recognise and foster awareness of the threat posed by criminals and terrorists at each point in the supply chain?				
1.14	Personnel should only be given access to those areas needed for the performance of their duties. Guard should check employees ID to monitor access to the restricted areas.				
1.15	Does the facility select and hire contractors (including other manufacturers, product suppliers, and vendors) to perform services?				
1.16	In selecting the contractors used by the facility, does the facility consider the contractors' security controls, financial stability, and corporate history?				
1.17	Does the facility have written security standards and documented procedures for its contractors?				
1.18	Do contractors that have access to restricted areas undergo a background investigation?				

Part 2 – Physical Security

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
2.1	Do management or security personnel control the issuance of all locks and keys?				
2.2	Does the facility have an alarm system and video surveillance cameras? Is there a back-up power source for the alarm system?				
2.3	Is there a procedure in place to identify challenges and address unauthorized/unidentified person?				
2.4	Are all buildings in the facility constructed of materials that prevent unlawful entry?				
2.5	Are all buildings thoroughly inspected, maintained and repaired so that there are no open areas through floors, roofs, or broken walls?				
2.6	Are perimeter barriers, fences and gates regularly inspected, properly maintained and repaired? If yes, check the records.				

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
2.7	Is there adequate lighting inside and outside the facility including entrances and exits, cargo handling and storage areas, fence lines and parking areas?				
2.8	Does the facility store containers/trailers onsite? If yes, do they store in a secure area with mechanisms in place to prevent unauthorized access?				
2.9	Are loaded stored containers/trailers sealed with security seals that meet or exceed industry standards?				
2.10	Does the guard force staff work in the facility 24hours a day, 7days a week? If yes, record the working time and shifts.				
2.11	Do security guards log incidents and report any security violation incidents to management personnel?				
2.12	Does the facility have a proper communication mechanism (e.g., phone, radio) to local police?				
2.13	Are gates for employees and vehicles entrance/exit guarded and/or monitored during operations and non-operating hours?				
2.14	Does access control include the positive identification of all employees, visitors, and vendors at all entry points? Check the records.				
2.15	Does an authorised employee escort visitors and vendors through the buildings?				
2.16	Are all visitors monitored while accessing restricted areas (e.g., loading/unloading, Operations Centre, IT, Finance)?				
2.17	Do guards patrol the interior of buildings in the facility? If yes, check the records.				
2.18	Are closed circuit television cameras (CCTVs) used to monitor activities inside/outside the facility?				
2.19	When are CCTVs monitored? Who monitors CCTVs? Is access to CCTV monitors controlled?				
2.20	Are there written procedures in place to stipulate how seals are controlled and affixed to loaded containers, including recognizing and reporting compromised seals and/or containers to management and authorities?				
2.21	Are vehicles prohibited/prevented from parking near cargo conveyances/perimeter fencing?				

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
2.22	Are parking lots for visitors separate from those for employees? If allowed to enter the facility area, are vendor and visitor vehicles inspected?				
2.23	Are there security measures in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in the supply chain?				

Part 3 – Storage and Distribution

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
3.1	Does the facility have fencing or other barrier materials to enclose cargo handling and storage areas to prevent unauthorised access?				
3.2	Is high value cargo marked, segregated, and stored separately within a fenced area or secure room?				
3.3	Is dangerous cargo, including hazardous material secured and stored separately and labelled when necessary?				
3.4	Is the loading and departure of containers/trailers supervised by a security officer or other designated supervisor?				
3.5	Are security controls in place to prevent unauthorised materials at the point of loading?				
3.6	Are cargo units identified, labelled, weighed and/or counted before loading?				
3.7	Is there a documented procedure in place to ensure that management and/or customs and/or local police are informed of all anomalies found in shipments?				
3.8	Are accurate, legible and complete cargo documents and packing slips prepared?				
3.9	Are there documented procedures for tracking goods for shipment? How to track?				
3.10	Are documented procedures in place to verify the integrity of the container structure through inspection of front wall, left side, right side, floor, ceiling/roof, inside/outside door, outside/undercarriage? Check the records.				

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
3.11	Is there a documented procedure to affix a security seal which meets or exceeds industry standards?				
3.12	Is there an individual responsible for issuing and tracking seals? Are there documented procedures for affixing, replacing, recording and tracking the seals placed on containers, trailers, and trucks?				
3.13	Does the facility keep records of seal numbers together with vehicle number, driver name, time and date of loading or unloading, container/cargo conveyance numbers? How long are the records kept?				
3.14	Are seal numbers verified at the time of the final sealing before departure?				

Part 4 – Shipping Information Control

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
4.1	Is there a designated company representative responsible for providing accurate information on the facility products to the forwarder and carrier?				
4.2	Are records maintained for all shipments?				
4.3	Are the information requirements automated?				
4.4	Does the responsible company representative understand the need to provide an accurate shipper, forwarder, and con-signee information? And the timeframes required for the advance information?				
4.5	Is the information requested in this section related to shipping records documented and verifiable?				

Part 5 – Information Security

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
5.1	Does the facility have pre-defined rules for access to information and does the facility have documented procedures for identifying which employee(s) are allowed access to electronic information system, facility documents, shipping forms, shipping data, shipping/cargo movement, security seals and, is there a name list of access limit?				

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
5.2	Does the facility have electronic information systems used for operational purposes? Is it password protected?				
5.3	Is access to the server room controlled and is there a procedure to control facilities in shared server rooms?				
5.4	Are relevant employees provided with individually assigned IT system accounts?				
5.5	Is there any password policy in-place and: - Does it require complexity, minimum length, and regular changes? Is it enforced in a systematic manner?				
5.6	Is there a designated system administrator who sets up user IDs and is there a procedure in place to deliver the password to the user in a secure manner?				
5.7	Is there an account lockout policy in-place to suspend an account after a certain number of failed attempts?				
5.8	Do desktops automatically lock after a designated period of inactivity?				
5.9	Are security logs kept and reviewed periodically for invalid password attempts and file access and are these logs stored based on a defined retention policy to meet regulatory requirements?				
5.10	Has the facility implemented the next generation Firewall on their network boundary? And: - Is there Intrusion prevention system in place? - Is there Anti-Virus installed on all computers? Are they all kept up to date?				
5.11	Is there a backup plan in place to save computer information /data in a backup system and are backup data transferred to a secure place such as fire resistance safe or off-site facility?				
5.12	Is there a tested plan defined to restore data in the case of failure?				
5.13	Is the information requested in this section related to IT security documented and verifiable?				
5.14	Are all information and operating systems getting vendors' updates/patches regularly?				

Part 6 – Records and Documentation

Serial	Checkpoints	Yes	No	N/A	Findings /Remarks
6.1	Does the facility have a documented policy that requires all security procedures to be documented?				
6.2	Does the facility have a designated manager/person responsible for overall site security?				
6.3	Is there a designated security department/team at the facility?				
6.4	Is there a person responsible for facility security, personnel security, contractor security, conveyance/transport security?				
6.5	Is there a person responsible for carrying out security audit risk assessments?				
6.6	Has any (internal, second or third party) site security assessment been conducted?				
6.7	Is there a documented procedure to conduct periodic security checks to ensure that the security procedures are being performed properly?				
6.8	Is there a documented security improvement plan that summarises or identifies vulnerabilities and responsive corrective actions?				
6.9	Is the facility security plan reviewed and updated periodically?				
6.10	Is the information requested in this section documented and verified?				

Part 7 – Facility Photos

This section provides useful photos for reference and audit confirmation.

Facility entrance	Auditor in front of facility
(Expand boxes and insert photos)	
Perimeter fencing	Facility building

Employee parking	Visitor Parking
Outside lighting	Security room – Communications equipment
CCTV system and monitors	Packing area
Loading area	Business licence
Facility security plan	Personnel security guidelines for hiring and terminating.
Personal file	Job description of a security guard
Work Handbook Rules	Visitor / vehicle in out access control record
Records of distribution of keys, codes, cards	Facility ID return and missing records
Transportation driver's entry-exit log	Screen records of arriving packages and mail

Container integrity inspection records	Container security inspection records
Cargo loading records	Seal control records
Internal periodic unannounced security check records	Industry standard certification

Part 8 – Corrective Action Plan

Section	Finding description	Corrective action agreed/planned	Implementation date	Remarks

B References:

- Cyber Essentials:
  https://www.cyberessentials.ncsc.gov.uk/

- Supply chain cyber protection guidelines on NCSC and CPNI:
  https://www.ncsc.gov.uk/collection/supply-chain-security
  https://www.cpni.gov.uk/supply-chain

- Verify suppliers on The NCSC website:
  https://www.ncsc.gov.uk/section/products-services/verify-supplier?q=&defaultTypes=organisation&sort=date%2Bdesc&start=0&rows=20

- NCSC Cyber Security Training for staff:
  https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

- NCSC – Exercise in a box
  https://www.ncsc.gov.uk/information/exercise-in-a-box

- ICO – Information related to data privacy & GDPR
  https://ico.org.uk/
  https://www.ncsc.gov.uk/information/GDPR

- Guidance related to NIS legislation and Cyber Assessment Framework:
  https://www.cpni.gov.uk/network-and-information-systems-nis
  http://www.legislation.gov.uk/uksi/2018/506/contents/made
  https://www.ncsc.gov.uk/collection/caf/nis-introduction

oguk.org.uk/guidelines

OGUK Guidelines
Member companies dedicate specialist resources and technical expertise in developing these guidelines with Oil & Gas UK with a commitment to work together, continually reviewing and improving the performance of all offshore operations.

Guidelines are free for our members and can be purchased by non-members.

oguk.org.uk

info@oguk.org.uk

@OGUKEnergy

OGUK

OGUK