PORT FACILITY SECURITY INSTRUCTIONS

PROTECTION CATEGORY: CRR

RESTRICTED

CONTENTS PAGE

Annexes

PFSIs contain detailed information about security measures in ports, and as such this document has been marked as "RESTRICTED". This is a Government classification and means that any document bearing such mark should only be read by security vetted staff and on a "need to know basis".

CHAPTER 1: INTRODUCTION

Part 1: Background

Since the terrorist attacks in the USA in 2001 the threat to transport systems world-wide has changed, including that to maritime transport. This has been acknowledged both nationally and internationally and has prompted the development of new and improved security regimes across the transport systems.

The International Maritime Organisation (IMO) responded to the attacks of September 2001 by developing new security requirements for ships and port facilities to counter the threat of acts of terrorism. These requirements took the form of amendments to the Convention on the Safety of Life at Sea 1974 (SOLAS) and a new International Ship and Port Facility Security Code (ISPS Code). The SOLAS amendments and ISPS Code were formally adopted in December 2002 and came into force on July 1, 2004, the same date that it was implemented by Jamaica.

The IMO requirements apply to passenger ships (including high-speed craft), cargo ships over 500 gross tonnes and Mobile Off-Shore Drilling Units (MODUs) engaged on international voyages, and the port facilities that service them. Additionally, the ILO/IMO Code of Practice on Security in Ports is used as universal guidance by States.

PAJ being the Designated Authority (DA) in Jamaica has overall responsibility for the policy development and implementation of the programme and has oversight responsibility for port facilities and the Maritime Authority of Jamaica has responsibility for ship security consistent with their mandate for port State control

Part 2: Legal Requirements

Although the IMO requirements are comprehensive, they do not set out specific security standards. It is considered that such standards are necessary in Jamaica to ensure effective security that is consistent across the various sectors of the ports industry.

The Port Security By-Laws, contained within the Port Authority Act, provides a mechanism by which these IMO security requirements are legislated locally for port facilities and port areas.

Part 3: Port Facility Security Instructions

The purpose of these Port Facility Security Instructions (PFSI) is to provide detailed instruction and guidance on the implementation of the required security measures, and the preparation of a Port Facility Security Plan (PFSP). This PFSI is not a legal document but aims to provide easy-to-follow guidance on local and international legal requirements.

It is important to note that the PFSI contains both information on legal requirements, and guidance and recommendations. Where information is for guidance purposes only, this is made clear in the text. Legal requirements are generally written using the phrase "shall", while guidance uses the phrase "should". Furthermore, Annex A lists all mandatory measures and gives a précis of the requirements. For detailed explanations refer to the relevant section of the main body of this document. The PFSI will be updated on the basis of experience and feedback as well as in response to changes in the overall security environment. When changes to the PFSI are purely minor textual amendments these will be made without notification. However, when changes are more substantial PFSOs will be informed of the changes by e-mail or by letter where e-mail is not available.

Part 4: Port Facility Security Plan Template

In order to assist Port Facility Security Officers in ensuring that their PFSPs meet the necessary legal requirements, and to ensure rapid and effective approval of plans by the National Accreditation Committee (NAC), a PFSP template has been developed that should be used by all port facilities when drawing up their plans. The headings in this PFSI correspond with those in the PFSP template to ensure completion of the plan is as simple as possible.

Complying with the PFSP format, these instructions and the accompanying security standards will help the industry to meet the IMO requirements and offer the best opportunity for preparing and submitting an acceptable PFSP.

A PFSP may cover more than one port facility if the operator, location, operation, equipment and/or design of the port facilities are similar and if this has been agreed in advance with the DA. In such cases the DA would recommend that each port facility has its own Security Chapter, each constructed around the PFSP template, which when taken together would constitute an overall port estate plan.

CHAPTER 2: SECURITY OVERVIEW

Part 1: Security Levels

The ISPS Code introduces an international system of three Security Levels:

Security Level 1: Normal
Security Level 2: Heightened
Security Level 3: Exceptional

These Security Levels reflect the likelihood that a security incident will occur; the higher the Security Level the greater the likelihood of a security incident. The Security Level above SL 2 will be set by the Minister with responsibility for Transport in conjunction with the Minister with responsibility for National Security. It will be communicated through the DA to all relevant port facilities; the Maritime Authority of Jamaica, the JDF Coast Guard, Marine Police and vessels which have signalled their intention to call at a Jamaican port.

At Security Level 1, port facilities will be required to have baseline security measures in place. Security Level 2 represents a heightened level of threat, and port facilities will be required to increase their levels of protective security. Security Level 3 represents an imminent and specific threat, and port facilities will be required to increase their security provisions still further and respond to instructions from the DA and relevant national security control authorities.

The specific actions and measures required at each Security Level must be detailed in each port facility's security plan. Port facilities must ensure that revised measures are in place immediately upon notification of a change in Security Levels and the plan must detail how the port facility will meet the increased commitments, for example by the redeployment of staff.

To introduce a greater degree of flexibility whilst maintaining the internationally mandated three (3) Security Levels, the DA has introduced a range of search percentages at each level. Ports and ships will be notified of the appropriate search percentage in the same way as changes to the Security Level. It is important to note that search percentages will reflect changes in threat assessments and/or specific risk analysis. Search percentages will not be arbitrary but will be set at pre-defined intervals of no less than 5%. This should allow port facilities to make business continuity decisions on allocation of resources and the need to arrange contracts with security providers among other arrangements.

This flexible approach will also allow DA/industry to enhance certain aspects of the security system, for example increasing the search percentages, without moving formally between the Security Levels. This capability will reduce the overall impact on the port facility, because the port facility will not be required to meet the full panoply of additional requirements, for example the continuous monitoring of CCTV feeds, that are necessitated by a formal increase in Security Level.

Part 2: Risk Assessment

Risk can be defined as a function of threat, vulnerability and consequence. Threat is a function of both the capability and intent of a terrorist group to mount an attack on a target; it varies from group to group, by target and over time. Vulnerability is the susceptibility of a target to a given form(s) of attack, and consequence is the impact and effect of a successful attack. Risk assessment is the means by which threat, vulnerability and consequence are identified and evaluated.

Threat is determined by threat assessment, i.e. the identification and evaluation of capability and intent. Threat assessment is dependent on intelligence data. Due to the nature of the available intelligence, threat assessments are rarely specific and are often expressed in generic terms using a system of threat levels.

Part 3: Security Measures and Standards

The aim of protective security measures is to reduce the risk to each port facility to an acceptable level, thereby reducing the overall risk to the maritime sector. Therefore, those port facilities where the risk is assessed to be greater will be required to implement more stringent security measures than those where the risk is lower.

It is important to note that the standards set by the DA are minimum standards and port facilities are free to implement higher standards and additional measures. However, where a standard has been specified in these instructions and a port facility chooses to work to a higher standard, this must be agreed in advance with the DA. It is also strongly recommended that port facilities wishing to implement additional measures seek advice from the DA on their suitability and applicability.

CHAPTER 3: MANAGEMENT OF SECURITY

Part 1: Port Security Committees – Part A Sec1.2.1 & 1.2.3

Guide to Maritime Security and the ISPS Code-2012 Edition-3.9.3-8

Port Security Committees (PSCs) are considered an essential part of any security regime, allowing all relevant stakeholders the opportunity to discuss security issues thus ensuring a consistent approach. This is particularly important when a port facility forms part of a wider port estate consisting of a number of different port facilities.

All port facilities must be a part of a PSC, which is required to meet no less than four (4) times a year and more often if necessary. At Security Levels 2 and 3 the DA may require them to meet on a more regular basis.

The role of the PSC will include, but will not be limited to:

- Co-ordinating implementation of the security measures required by the PFSP(s);
- Ensuring consistency and compatibility of approach within the port estate; and
- Providing feedback on implementation, exercises, testing, training and updating of the PFSA and PFSP.

Membership of the PSC must be open to all representatives with a security responsibility within the port, to the statutory controlling authorities and other interested parties as appropriate. However, the membership must include the PFSO, Deputy or nominated representative of each port facility within the port estate. It may also include representatives from:

- Jamaica Defense Force -Coast Guard (JDFCG)
- Jamaica Constabulary Force (JCF)
- Shipping Agents
- Jamaica Customs Agency (JCA)
- Passport Immigration and Citizenship Agency (PICA)
- Trade Union and/or Workers Representatives
- Other port users (as appropriate)

Wherever possible, PSCs should be set up and chaired by the PFSO.

Part 2: Security Level Changes

The DA would advise port facilities of changes to Security Levels.
PFSO’s must ensure that they, or a designate, can be contacted on a 24-hour basis.

Port facilities are required to ensure that procedures are in place for advising relevant staff of changes to Security Levels. Port facilities must ensure that

revised measures are in place immediately upon notification of a change in Security Level.
Confirmation must be provided to the Vice President and/or Assistant Vice President of Security of the DA that this has been achieved. See Annex A.

Part 3: Security Duties of Port Facility Personnel

Port Facility Security Officer (PFSO) – Part A Sec 17.1 -17.3

All port facilities must have a PFSO who has been suitably **vetted trained and certified**. A person may be designated as the PFSO for more than one port facility. Where several port facilities fall within the same port estate, a PFSO may be appointed to cover them all. However, when designating a PFSO, port facility operators should consider the practical implications and the level of authority and responsibility that would be required of a PFSO designated for more than one port facility.

Port facility operators are strongly advised to designate deputy PFSOs to ensure continuous cover during periods of absence.

A PFSO/Deputy’s appointment **cannot** be confirmed until the DA is satisfied that the person nominated is suitably qualified in accordance with the training requirements outlined in Part B 18.1, of the ISPS Code, and IMO Circular1188, hence, is able to perform the duties outlined in Part A 17.2.

The duties of a PFSO must include:

- Conducting an initial comprehensive security survey of the port facility, considering the relevant PFSA;
- Ensuring the development and maintenance of the PFSP;
- Implementing and exercising the PFSP;
- Undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;
- Recommending and incorporating, as appropriate, modifications to the PFSP to correct deficiencies and to update the plan to take into account relevant changes to the port facility;
- Enhancing security awareness and vigilance of the port facility personnel;
- Ensuring adequate training has been provided to personnel responsible for the security of the port facility;
- Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;
- Co-ordinating implementation of the PFSP with the appropriate Company and Ship Security Officer(s);
- Co-ordinating with the DA and control authorities, as appropriate;
- Conducting audits of the PFSP;
- Ensure that security drills and exercises are conducted according to timelines outlined in the ISPS Code;

- Ensuring that standards for personnel responsible for security of the port facility are met;
- Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any;
- Assisting Ship Security Officers in confirming the identity of those seeking to board the ship when requested; and
- Organising and Chairing Port Security Committee meetings as appropriate.

PFSOs must be given the necessary support, time and resource to fulfil the duties and responsibilities outlined above. Therefore, although PFSOs may have other, non-security related duties, these must not interfere with the PFSO's ability to undertake their security duties.

Other Personnel with Security Duties – Part A 18.1 & 2

All port facility personnel with security duties or responsibilities must have sufficient knowledge and ability to perform them. The PFSO must also ensure that performance measures are in place to allow the effectiveness of staff undertaking security duties to be assessed.

Examples of personnel with specific security duties include:

- search staff;
- patrol / static guards;

In addition, all staff with security responsibilities must be subject to employment checks prior to confirmation of appointment. Such checks should include consideration of at least two references and a police criminal record check.

All Other Port Facility Personnel – Part B 18.3

All other port facility staff must receive security awareness training. Although there is no expectation for these staff to become security experts, an intrinsic part of Jamaica's approach to the implementation of the ISPS Code is the engendering of a security culture throughout the ports sector. Increased security awareness will improve the overall security of your business by increasing its monitoring capability. All staff should be encouraged to report persons behaving suspiciously.

Part 4: Vetting of Port Facility Personnel

All regular port users must undertake, at a minimum, a Criminal Records Check and provide evidence of such prior to issue of a permanent pass. This applies to all persons with security responsibilities.

Part 5: Security Training

Port Facility Security Officer (PFSO)-Part B 18.1

All PFSOs must attend a PFSO training course and pass the assessment that forms part of the course.

Personnel with Security Duties- Part B 18.2

Port facility personnel with specific security duties should have knowledge and receive training in some or all the following, as appropriate:

- Knowledge of current security threats and patterns;
- Recognition and detection of weapons, dangerous substances and devices;
- Recognition of characteristics, and behavioural patterns of persons, who are likely to threaten security;
- Techniques used to circumvent security measures;
- Crowd management and control techniques;
- Security-related communications;
- Operation of security equipment and systems;
- Testing, calibration and maintenance of security equipment and systems as appropriate;
- Inspection, control and monitoring techniques;
- Methods of physical searches of persons, personal effects, baggage, vehicles, cargo and ship's stores; and
- Bomb threat assessment procedures.

It is particularly important for staff with search responsibilities to be trained in search techniques to ensure effective searching. Search training should encompass techniques for searching people, bags, all vehicles (including cars, vans, coaches, motorcycles, pedal cycles, caravans and trailers) and must include training in the operation of any equipment provided as an aid to searching. Search personnel should also have an adequate level of understanding of weapons and devices and refresher training should be undertaken on a regular basis.

Other Personnel - Part B 18.3

Ports will be required to provide security awareness training for all their employees. This will be in keeping with **Part B18.3** of the ISPS Code's recommendation that all port facility staff receive security awareness training. The DA believes that a basic understanding of security issues by all port facility staff will greatly improve the effectiveness of the port facility's security regime.

An effective security regime relies on the vigilance and awareness of all those employed by, and present at, the facility in question. Port facility operators must therefore provide basic awareness training to ensure that all employees have knowledge of and are familiar with relevant provisions of the PFSP and some or all the following, as appropriate:

- The meaning and consequential requirements of the different security levels;
- Recognition and detection of weapons, dangerous substances and devices;
- Recognition of characteristics and behavioural patterns of persons who are likely to threaten security; and
- Techniques used to circumvent security measures.

There is no expectation that these personnel should become security experts and security awareness training may be combined with existing induction or health and safety training if security is addressed as a specific item and all relevant security issues are covered appropriately.

Port facility operators are also encouraged to make security awareness training available to all other staff working at the port facility, even if they are not direct employees, including contractors, regular suppliers and to encourage companies whose staff work at the port facility to supply such training themselves.

<u>The objective of these layered training requirements is to engender a security culture whereby every member of staff can contribute to the overall security of the port facility.</u>

Staff awareness can be achieved in several ways, examples of which are outlined below:

- Staff can be briefed on security issues by the PFSO as part of the general orientation/ training of new employees.
- Regular reviews and informal training sessions can be held.
- All staff can be involved on a rotational basis with the Drills and Exercises that the port facility is required to run.
- The PFSO can hold quarterly security awareness briefings at the facility. This may be achieved by way of staff notices, formal training, newsletters, signage, etc.

Part 6: Security Drills and Exercises – *Part B 18.4- 18.6*

Forms for running drills/exercises and for reporting on their completion are at Annexes K and L.

Security drills and exercises are designed to ensure that port facility personnel are proficient in all assigned security duties and at all Security Levels. In addition, practice will identify any security-related procedural and / or physical deficiencies that need to be addressed.

Security drills and exercises may be combined with other exercises, such as safety evacuation drills of a Local Authority or contingency planning exercises, if the drill / exercise scenario contains a security element. For example, an evacuation drill could be prompted by a bomb threat warning, and security personnel would then have to use the bomb threat checklist, confirm procedures for contacting the police and conduct a search of the port facility (security sweep) to check the veracity of the warning. Multi-purpose drills and exercises have the benefit of increasing inter-agency co-operation and familiarity with external procedures.

Drills

To ensure the effective implementation of the provisions of the PFSP, drills should be conducted as follows:

1. At **least** once every three months.
2. Prior to the resumption of activity at a port facility that has been inactive for more than three months.
3. Prior to the start of business at a port that has been newly certified.

The specific timing of drills should consider changes of port facility personnel, the type of ship the port facility is serving and the operations conducted at the port facility. This will ensure that personnel can carry out their duties in all operating conditions.

These drills will generally involve small-scale testing of individual elements of the security plan. Examples of drills include:

- Carrying out an evacuation;
- Requiring the pass issuing officer to run through the procedures to be followed if a pass is lost;
- Requiring a member(s) of staff to use the bomb threat checklist to replicate a bomb threat;
- Response to a breach of a Restricted Area or Controlled Building;
- Running through procedures for the identification of suspect vehicles with security guards; or
- Response to the discovery of a suspect package or weapon on a person.
- Communication drill verifying the contact details of state and response agencies.

In addition to the above examples, port facility staff with security responsibilities must be adequately drilled to ensure that they can respond effectively to an increase in the Security Level. This is particularly important with respect to those staff members who are only activated for security purposes at Level 2. This should include at least one hypothetical Security Level amendment a year.

Exercises

Various types of exercises, which may include participation of PFSOs, in conjunction with relevant control authorities, CSOs or SSOs, if available, should be carried out at least once each calendar year, not exceeding eighteen (18) months. Requests for participation of CSOs or SSOs in joint exercises should be made bearing in mind the security and work implications for the ship. These exercises should test communication, co-ordination, resource availability and response. This should include the substantial and active participation of personnel with security responsibilities.

Exercises may be:

- Full-scale and live;

- Tabletop simulation or seminar; or
- Combined with other exercises held, such as emergency response or other Government authority exercises;

and may cover the following types of security incident:

- Damage to, or destruction of, the port facility or of the ships, e.g. by explosive devices, arson, sabotage or vandalism;
- Hijacking or seizure of a ship or of persons on board;
- Tampering with cargo, essential ship equipment or systems or ship's stores;
- Unauthorised access or use, including presence of stowaways;
- Smuggling weapons or equipment, including weapons of mass destruction;
- Use of the ship to carry those intending to cause a security incident and their equipment;
- Use of the ship itself as a weapon or to cause damage or destruction;
- Blockage of port entrances, locks, approaches, etc.; and
- Nuclear, biological and chemical attack.

Exercise Evaluation

The Designated Authority, The Port Authority of Jamaica, must be represented at the exercise to evaluate the effectiveness of the exercise to determine if both the national, and international requirements of the *ISPS Code Part B 18.6* have been satisfied.

The DA reserves the right to determine whether an exercise was appropriately conducted, and if the exercise fails to meet the requirements, to mandate that another one be held within three (3) to six (6) months.

Part 7: Security Equipment Maintenance

The type and variety of security equipment will vary depending on the nature, layout and resources of the port facility. However, regardless of equipment type or the extent to which it is used, all security equipment must be subject to regular maintenance checks.

Security equipment includes but is not limited to:

- Fencing
- CCTV
- Lighting
- Communications systems
- X-ray equipment
- Archway Metal Detectors (AMD)
- Hand Held Metal Detectors (HHMD)
- Perimeter / Intruder Detection Systems (PIDS/IDS)
- Automated Access Control Systems (AACS)

- Explosive trace detection equipment
- Vapour detection equipment
- Under Vehicle Video (UVV)
- Underwater Surveillance Vessel (USV)

Where deficiencies are noted, and repairs are required, contingency procedures should be in place to implement back-up or temporary systems until repairs have been completed. For example, when a CCTV system used to monitor a Restricted Area ceases to function, adequate monitoring could be maintained by increasing the frequency of security patrols. The DA should be informed if any security equipment is out of service and may compromise security.

Part 8: PFSP Review, Amendment and Audit– *Part B6.58- B16.60*

PFSP Review and Amendment

It is the responsibility of the PFSO to review the PFSP, and the procedures, requirements and activities laid down in it, on a regular basis but at least every six (6) months. The PFSP must also be reviewed under the following circumstances:

- The relevance of the PFSA has been affected by operational changes at the port facility;
- An independent audit of the PFSP or a -DA inspection of the port facility identifies failings in the organisation or questions the continuing relevance of significant elements of the approved PFSP;
- Following significant weaknesses identified in the security systems and/or procedures after a drill or exercise;
- Following a security incident or threat thereof involving the port facility; and
- Following changes in ownership or operational control of the port facility.

The PFSO can recommend appropriate amendments to the PFSP following any review of the plan. However, where amendments relate to any of the following, the PFSP must be submitted to DA for consideration and (re-)approval:

- Proposed changes which could fundamentally alter the approach adopted to maintaining the security of the port facility; for example, change in nature of port facility operations including the removal or alteration of permanent barriers, security and surveillance equipment and systems, etc and/or building works considered essential in maintaining the security of the port facility.

PFSP Audit – Part B16.3.5

The PFSP should be audited internally at least bi-annually. Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation must be independent of the activities being audited unless this is impracticable due to the size and nature of the port facility.

In addition, PFSPs may be audited at any time by the DA

PFSP Re-certification

All ISPS certified ports are required to be re-certified every five years. To initiate this process, it is the responsibility of the port management to have Port Facility Security Assessments and Plans prepared and submitted to the Port Authority of Jamaica for evaluation and approval.

To complete the re-certification process in a timely manner, it is required that the PFSA and PFSP are submitted for consideration and approval at least **six months** and **three months** respectively prior to the due date of re-certification.

Part 9: Security Incident Reporting and Assessment – Part B 16.3.6

Port facilities are required to have security incident reporting systems in place, which must be detailed in the PFSP. These systems must cover two aspects of incident reporting:

- Enabling port facility personnel to report security incidents at the port facility (internal reporting).
- Enabling PFSOs and port facility operators to report security incidents to the DA and other relevant authorities.

The primary aims of port facility incident reporting systems are:

- To identify deficiencies in protective security measures.
- To provide a means of monitoring the number and types of security incidents and occurrences that could endanger maritime security.
- To enable the DA to assess whether trends revealed by the reporting system affect the threat to maritime security.
- To enable the DA to respond to any media interest in an incident.

Internal Reporting

All staff must be aware of the procedures for reporting security incidents. These procedures should be simple to follow and should in no way discourage reporting.

The PFSO is responsible for investigating all reported security incidents occurring on their facility. The PFSO is also responsible for ensuring that any necessary remedial action is undertaken.

Reporting to the Designated Authority

The DA is responsible for the monitoring of security incidents and occurrences that could adversely affect maritime security and has an interest in the investigation of the circumstances surrounding the incident and the remedial action required.

Any security incident which occurs on a vessel in Jamaica's territorial waters or on a Jamaican flagged vessel in international waters, or a vessel whose last or next port of call is in Jamaica, must be reported to the DA immediately on receipt of the information.

The types of incident that must be reported to the DA are outlined briefly below. It should, however, be noted that incident types have been kept relatively general to provide the PFSO or port facility operator with a degree of flexibility in making considered judgements. To list every conceivable type of incident would be impractical and serve little purpose.

Based on the foregoing it is required that the PFSO submit a monthly report to the PAJ Security Department for the attention of the Vice President of Security. If there are no incidents to report this must also be communicated.

The priorities and timelines for reporting incidents to the DA vary depending on the incident type and these are outlined below and listed in Table 1. However, it is important to note that the timelines provided are the latest times for reporting an incident and do not preclude earlier reporting.

Bomb warnings

All bomb warnings must be reported immediately to the DA In addition, the total number of such incidents must be included in the monthly report to the DA. Port facility operators must retain a full record of each incident to inform possible future prosecution of the offender.

Bomb Threat Assessment

To respond appropriately to a bomb threat training is necessary. The port facility must therefore ensure that coordination with local bomb threat assessors is in place.

A bomb threat checklist, for use by any person receiving a bomb threat, can be found at Annex D.

Hijack

The hijacking of any vessel of interest to the DA must be reported immediately on receipt of such information.

Discovery of firearms and ammunition

Once an undeclared firearm is discovered onboard a vessel this must be reported immediately to the DA and the police.

Discovery of weapons other than firearms

This incident type covers the discovery of items that could be used by an individual to endanger the security of the port facility, a ship within the port facility, ship and port facility personnel, passengers or crew. Such items include knives, volatile fluids etc. Details of such items are included in Annex H - List of Prohibited Items.

Where the discovery of weapons other than firearms involves suspicion that their carriage was intended for the purpose of endangering passengers, crew or the vessel, and further action is initiated, this should be reported **immediately**. In all other cases such occurrences need only to be reported on an aggregated monthly basis.

Discovery of explosives

This incident type includes the discovery of the component parts of an explosive device such as the detonator. Discovery of undisclosed explosives must be reported to the DA immediately.

Where the discovery of such components involves suspicion that their carriage was intended for the purpose of endangering passengers, crew or the vessel, and further action is initiated, this should be reported immediately. In all other cases such occurrences need only to be reported on an aggregated monthly basis.

Unauthorised access to Restricted Areas or Controlled Buildings

This incident type covers all cases when an individual gains unauthorised access to a Restricted Area or Controlled Building within a port facility or on a ship when in a port facility.

Where unauthorised access involves suspicion that access was intended for the purpose of undertaking illicit activity, this should be reported immediately. In all other cases such occurrences need only to be reported on an aggregated monthly basis.

Incidents of which the media are aware

If the media become aware, or are believed to be aware, of an incident or occurrence, it is important that the DA is notified immediately

Other Significant incidents

This incident type covers any incidents or occurrences that do not fall under the types outlined above but which are considered by the port facility operator or PFSO to be of such significance as to be reported to the DA immediately. These may include industrial unrest, explosions, discovery of hazardous material and threat to the environment.

Miscellaneous incidents

No reporting priority is given for miscellaneous incidents. Timelines for reporting are left to the discretion of the port facility operator or PFSO.

Table 1: Incident Reporting Priorities

Incident Type	Immediate notification	Notification within 24 hrs	Monthly Report
Incidents of which the media are aware	√		√
Bomb warnings: Credible	√		√
Hijack	√		√
Discovery of firearms and ammunition Suspicious Routine	√		√
Discovery of other weapons Suspicious Routine	√		√
Discovery of explosives: Suspicious Undisclosed Disclosed	√		√
Unauthorised access to restricted areas: Suspicious Routine	√		√
Other Significant incidents	√		
Miscellaneous incidents	(as considered appropriate)		

Where more than one individual or company is involved in an incident or occurrence, all individuals, companies and agencies involved are requested to submit reports. Multiple reports often provide a picture of the incident from a variety of viewpoints and can assist in a better understanding of the precise events.

Although it is difficult to use a single format for reporting given the variety of potential security incidents, suggested formats for written reports are included at Annexes B and C. These should be used wherever possible to enable rapid processing within the DA. Those incidents requiring immediate reporting should be reported initially by telephone to either the DA or, if out of hours, the Departmental Security Officer and followed up immediately with a written report.

The reporting of incidents and occurrences to the police is not affected by these procedures and should continue.

Part 10: Contingency Plans and Evacuation Procedures

All port facilities are required to develop contingency plans covering the following subjects:

- Bomb threat at the port facility or on a board ship (both in port and seeking to enter port)
- Procedures for conducting a bomb search at the port facility (or to facilitate a search on board a ship (if requested by the SSO, AMJ or Law Enforcement)
- Evacuation of ships or port facility property
- Action in the event of detonation of explosive or incendiary devices
- Other relevant situations

Contingency plans must include details of all actions to be taken, persons to be contacted and schematics of land and buildings affected. Copies should be made available to all parties involved. The plans should also consider:

- Numbers of staff required to instigate the plan
- Training requirements for appropriate staff
- Trials, drills and exercises to ensure the plan can be effectively implemented

Part 11: Information Security

Documents

Documents issued by the DA that carry the marking “Restricted” are security sensitive. "RESTRICTED" is a Government classification marking and there are specific rules about handling/storing documents bearing it. These documents must be kept under lock and key and away from general view when not in use. Information contained within these documents should only be passed to those with a strict need to know and only persons vetted should have direct access to the papers. Similar arrangements should be applied to documents created by port facilities that contain sensitive information relating to security procedures, including the PFSA report and the PFSP itself. Any sensitive information contained on IT systems should be accorded similar protection and should be password protected. Offices where sensitive information is stored should have a protective security system.

Cyber Security

Cyber security can be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

Cyber environment' comprises the interconnected networks of both information and cyber physical systems that use electronic, computer-based and wireless systems, including information, services and social and business functions that exist only in cyberspace.

In order to assess the risk that the port has in relation to cyber security the following questions must be considered:

1. Do you own, operate or occupy a port or port facility that has electronic or computer-based systems?
2. If the port systems were to fail, malfunction or were misused would this result in economic, operational, physical or reputational loss or damage, or disrupt operations?
3. Do you own an information asset that includes information about your strategy and/or commercial operations, the construction and/or operation of your port or port facility, including any port systems?
4. If this information asset were compromised could this result in economic, operational, physical or reputational loss or damage?

Physical defences against attack on electronic systems

Perpetrators of attacks range from individuals and organised groups of hackers through to organised crime, foreign intelligence services and terrorists.

The motivations (or 'actors') for a cyber-attack on a port system, can be for one of the following five purposes:

(a) espionage – seeking unauthorised access to sensitive information (intellectual property, commercial information, corporate strategies, personal data, pattern of life) and disruption for state or commercial purposes.

(b) activist groups (also known as 'hacktivism') – seeking publicity or creating pressure on behalf of a specific objective or cause, for example, to prevent the handling of specific cargos or to disrupt construction of a new port facility. The target may be the port itself, the operator of a port facility or a third party such as the supplier or recipient of the cargo.

(c) criminal – largely driven by financial gain, this can include criminal damage, theft of cargo, smuggling of goods and people, and attempts to evade taxes and excise duties.

(d) terrorism – use of the port to instil fear and cause physical and economic disruption.

(e) warfare – conflict between nation states, where the aim is disruption of transport systems/infrastructure to deny operational use or disable specific port facilities, such as bulk terminals.

Whilst there are a number of individuals and organisations identified as potential attackers the types of attack fall into four (4) categories:

1. Denial of Service (DoS) – this involves an attempt to render a system wholly or partially inoperative for a period of time. This is historically a remotely launched electronic “flooding” type attack. However, DoS could also be achieved by direct physical attack on key hardware or cables.

2. Corruption of Data – almost all historical evidence relates to remote attacks. E.g. hacking, malicious software (viruses) etc, although clearly insider actions is a possibility.

3. Theft or loss of Data – can be achieved via insider privilege abuse (either due to disaffection or coercion) or covert interception of electronic data flows. The latter has always to date been remote attack with no apparent need to gain physical access. Theft of data can also occur as a secondary (unintended) consequence of hardware theft depending on the efficacy of data back-up procedures.

4. unauthorised access to sensitive port data (commercial, personal or security related); (b) deletion, unauthorised modification or corruption of port data; (d) infection with malware; (e) loss of service from systems due to loss of connectivity or power; (f) loss of service from systems due to software and hardware failures; (g) compromise of port security systems; (j) jamming or interference with positioning systems (GNSS/GPS); and (k) assessing efficacy of system operation (for example, coverage and performance of CCTV and intruder detection systems).

Sources of attacks can be both internal and external to the organization.

- External attacks can be remote and clandestine, however they can also be effected by an attacker who has gained physical access to the facility’s infrastructure. From the attacker’s point of view this mode is attractive because it is cost effective, has reduced risk of arrest, allows plausible deniability (may be a disadvantage if an organisation wants to claim responsibility) and allows jurisdiction hopping (may be launched from other countries).
- Internal attacks originate within the organization. The “insider threat” is a generic term for a threat to the organization that comes from within – usually attributed to employees or former employees, but may arise from third parties such as contractors, temporary workers or customers. These can be categorized as malicious or accidental.
    - Accidental threats refer to situations in which damage or data loss occurs because of an insider who has no malicious intent. Examples are accidental deletion of important data, falling victim to a phishing attempt or inadvertently sharing data with an unauthorized party.
    - Malicious threats refer to deliberate attempts by an insider to access and potentially harm the organization’s data, systems or infrastructure. These are often attributed to disgruntled employees or ex-employees who feel wronged by the organization and seek

revenge. Insiders also become threats when they are subverted by malicious outsiders, either through financial incentives or extortion.

Some recommended mitigation activities for these types of risks are:

- Implementation of appropriate procedures when employees terminate their employment, with consideration given to the nature of their position and the level of access they hold;
- Ensuring effective policies and procedures for access and use of systems are in place and enforced, e.g. password policies, information sharing policies, acceptable system usage policies, etc.;
- Employee training and security monitoring;
- The use of spyware scanning programs, antivirus programs, firewalls, and a rigorous data backup and archiving routine.

The majority of attacks are remote and clandestine. From the attackers point of view this mode is attractive because it is cost effective, has reduced risk of arrest, allows plausible deniability (may be a disadvantage if an organisation wants to claim responsibility) and allows jurisdiction hopping (may be launched from other countries). The other main source of attack is from insiders.

Physical Protection

The physical element of attacks on systems is small, hence, to give proportionate guidance on physical defence it will be necessary to consider threat, vulnerabilities and consequences.

Covert physical access by outsiders in order to carry out, or increase the effectiveness of, e-attack is seen as a remote manifestation of the threat. More likely for this purpose is covert physical access by insiders. The physical response to the latter threat should be to ensure access control systems are in place limiting access to equipment, possibly by internal zoning, strictly to those with a legitimate purpose.

More likely action by outsiders than the covert access methods above is direct physical attack on electronic systems and this deserves consideration for protective measures.

The assets to be protected are, generally, cables (especially outside the guarded perimeter), servers and control rooms. The degree of protection would depend on the vulnerability of the system. For example, questions to consider are:

1. A network may be able to tolerate loss of one server but not two or more. Are these servers in the same location?
2. Is there a diversity of cable routes between key points?
3. How quickly can the assets be replaced and what are the consequences of delay? (Loss of some systems can have severe consequences within days).
4. Does a back-up system exist?

5. How often is data backed up?

The type of physical protective measures to be applied will be in line with those for other types of assets e.g. hardening of structures/containers, access control, perimeter security; and the scope should be extended to include coverage of those facilities essential to the function of the assets, e.g. cooling systems for the computer rooms and possibly power supplies dependant on the overall system resilience.

If a back-up system exists it should be ensured that the procedures for transfer of the operations are practised.

Part 12: Dangerous Goods and Hazardous Substances Procedures

It is essential that port facility operators are aware of any dangerous goods passing through the port facility and that procedures for handling and recording the transit of such goods are in place. Existing safety requirements (consistent with the International Maritime Dangerous Code, IMDG Code) provide a strong foundation on which to develop security requirements.

Part 13: Ships' Crew and Shore Leave

It is essential that the rights and needs of seafarers are considered throughout the implementation process and that security measures do not unduly inhibit seafarers' ability to access shore facilities, take shore leave and receive visitors. Port facility operators should pay particular attention to the needs of ships' crew when implementing pass systems and conducting searching. Ships' crew and their visitors should not be subject to more frequent or intrusive checks or searching than others requiring access to the port facility / Restricted Area(s) / ship. Ship’s crew are required to carry passports, Seafarer’s ID Card, or ship’s pass in order to exit or enter the port facility.

Part 14: Record Keeping – *Part B16.5*

The PFSO shall ensure that records or documents are kept for a period not under five (5) years and are protected from unauthorized access, but readily available for inspection at audits.

The PFSO shall keep the following records:

1. Records of security training including the date, duration, and description and the names of the participants.
2. Records of security drills and exercises including the date and description, the names of the participants and lessons learnt.
3. Records of security threats, breaches of security and security incidents including the date, time, location, and description and to whom they are reported.

4. Record of changes in the Security Level, date and time of notification and of compliance.
5. Records of maintenance, calibration and testing of security equipment, date and time of activity for each piece of equipment.
6. Declarations of Security (DOS).
7. Internal audits and reviews of security activities.
8. Reviews of the Port Facility Security Assessments (PFSA) and Plans (PFSP), with date, findings and recommendations, and date of approval and implementation.
9. Records of inspection and patrol.
10. List of names and positions of persons with security responsibilities.

Records may be kept in electronic format if they are protected from deletion, destruction and revision

CHAPTER 4: COMMUNICATIONS

Part 1: Ship and Port Facility Communication Links

It is important to ensure that there are effective channels of communication between the port facility and ships within, or intending to enter, the port facility. For example, it is essential that port facilities are aware of the Security Level of any ship intending to enter so that, where necessary, appropriate action can be taken.

It is also important to ensure effective communication between security personnel within the port facility. Effective communication will allow co-ordinated response to a security incident and is particularly important at Security Level 2 where both monitoring of the CCTV system and security patrols will be undertaken. Any person responsible for CCTV monitoring should be able to communicate with security patrols at all times.

There should be back-up systems or alternative means of communication for all essential communications. These systems may include hand-held VHF radios or mobile telephones.

Part 2: Ship Security Alert

Response to any criminal activity on the seas in Jamaican waters rests with the Marine Police and JDF Coastguard. Responsibility for investigation and prosecution of all offences committed in Jamaican waters rests with the Jamaican Police. (The Ship Security Alert System (SSAS), if activated in Jamaican waters will be received by the JDF Coast Guard on behalf of the Maritime Authority of Jamaica and the Coast Guard will determine in conjunction with the MAJ any required action).

Part 3: Declaration of Security – *Part A 5.1 – 5.7*

A Declaration of Security is a written agreement between a ship and a port facility, or a ship and another ship that confirms the security responsibilities of each party during the ship/port interface or ship/ship interface.

PFSOs are responsible for the administration of Declarations of Security (DOS) on behalf of the port facility. SSOs are responsible for DOS administration on behalf of a ship. However, where a ship does not have a SSO, for example where it is outside the scope of the ISPS Code, the DOS may be administered by the ship's master.

A DOS is <u>not</u> required for every vessel call.

Declarations of Security must be requested by PFSOs for all ships entering the port facility whenever the following circumstances apply:

- **Vessels entering Jamaican ports for the first time should be required to undertake a DoS**

- **When a non-SOLAS ship requires entry to a port facility.** In the case of ships below convention size, the decision as to whether a DOS should be initiated will depend on the type of vessel, its previous port(s) of call and whether it could have, for example, carried out a ship/ship interface at sea that involved transhipment. Advice on individual cases can be sought from the DA However, a DOS must be initiated whenever the port facility is at Security Level 2 or 3.

- **In all cases where the port facility or a ship entering the port facility is operating at Security Level 3.**

- **When a ship is operating at a higher Security Level than the port facility.**

- When the port facility is operating at an elevated security level

- **Following a security incident or security threat** to the port facility or ships operating within it, such as a bomb warning, the discovery of weapons/explosives, unauthorised access to the port facility, etc.

- **When requested by a DA Compliance Auditor.**

Port facilities and ships must co-operate with all requests for a DOS by a ship and/or port facility. Both parties must liaise to ensure that all measures required at the relevant Security Level are in place and are operating to a satisfactory standard.

The DOS must address the security requirements for the specific interface and detail what measures can be shared or should be provided, and by whom, in addition to those already in place.

If the Security Level of the ship or port facility changes during the operation of a DOS, the DOS must be reviewed and, where appropriate, amended.

Port facilities must retain a copy of each DOS for a period of three years and be able to make these available for inspection by PAJ (DA) compliance auditors upon request.

Suggested DOS procedures for port facilities

When the port facility requires a DOS the PFSO should:

- contact the SSO or ship's master prior to the ship's entry into the port facility;
- establish the Security Level of the ship(s) concerned and confirm the port facility Security Level;
- obtain details of security measures the vessel intends to carry out;
- draw up details of the security measures the port will put in place;
- agree measures with the SSO to ensure the highest Security Level is met;
- ensure the form of DOS in use by the vessel accords with the model attached (Annex E) as per the ISPS Code;
- complete the DOS for signature by both parties; and
- ensure retention of DOS for inspection.

When a ship requests a DOS the PFSO should:

- confirm the reason for the request and compare ship and port facility Security Levels;
- ascertain what security measures the ship has in place;
- agree the security measures the port facility will put in place, where appropriate;
- agree the details of such security measures with the SSO or ship's master;
- ensure the form of DoS in use accords with the ISPS Code;
- complete the DoS for signature by both parties; and
- retain the DoS for inspection.

Part 4: Response Agencies and Control Authorities

Port facilities must keep up to date contact details for all relevant response agencies and control authorities to ensure rapid and effective communication when necessary. Relevant agencies / authorities may include:

- Port Authority of Jamaica (PAJ);
- Jamaica Constabulary Force (JCF);
- Jamaica Customs Agency (JCA)Passport Immigration and Citizenship Agency (PICA)_Jamaica Defense Force (JDF)
- Ministry of Transport and Mining

- Ministry of National Security
- JCF -Marine Division

CHAPTER 5: SECURITY MEASURES

Part 1: Designated Restricted Areas – Part B 16.21- 16.29

The requirement to designate Restricted Areas within a port facility will be determined during the PFSA.

A Restricted Area can be designated anywhere within a port facility and in some cases may encompass the entire port facility. Although designation of Restricted Areas will vary depending on the specific assets, infrastructure and vulnerabilities of an individual port facility, the following areas will generally be classed as Restricted Areas:

- areas where dangerous goods and hazardous substances are stored;
- passenger berths / shore-side areas immediately adjacent to the ship;
- container freight storage areas;
- control authorities' check and search points; and
- essential electrical, radio and telecommunication, water and other utility installations.

Restricted Areas will, in most cases, be permanent and such areas will need to be delineated, secured and sign-posted. However, where a port handles a vessel, cargo or traffic type (as detailed in Chapter 6), but does so only on an infrequent basis, the Restricted Area may be temporary (albeit with the same characteristics i.e. signed and secured). Such circumstances are outlined in Part 2 below.

Port facilities must ensure that signs are displayed around the perimeter of Restricted Areas to make clear that access is prohibited unless a person has a recognised pass and has been liable to body/possession or vehicular search. It is recommended that signs be erected at even intervals along all stretches of the fence line, at changes of direction in the fence line and at access points. Signs must be clear, legible and prominently displayed either on the approach to the area or affixed to structures forming part of that area. Suggested wording for such signs can be found at Annex F.

The distance between Restricted Area signs has not been specified because the frequency that may be considered reasonable will vary from port to port and because, in many cases, port perimeters are punctuated with buildings or changes in the direction of the fence line. It is therefore for the port to determine what would be considered reasonable in accordance with its' specific circumstances. Details can be discussed during the PFSA visit or submitted as part of the PFSP and signage provision will be approved on a case by case basis.

Port facilities are required to ensure that access to Restricted Areas is not facilitated by the proximity of vehicles or any other item that could be used as a

climbing aid to help circumvent the fence. The requirement to maintain this "clear zone" around a Restricted Area remains constant irrespective of the prevailing Security Level.
Port facilities must erect signs along the berth face to warn approaching unauthorised vessels that they are in a restricted area and the consequences of the breach. – See Specifications in Annex….

At Security Level 2 consideration should be given to increasing the size of the "clear zone". Although the DA understands the constraints resulting from the size and shape of the port facility every effort should be made to increase the "clear zone" for example, by restricting vehicular access as outlined above. The "clear zone" is also intended to provide a clear line of sight to security staff and minimise the damage to the perimeter fence.

Part 2: Designated Temporary Restricted Areas

The requirement to designate Temporary Restricted Areas (TRAs) within a port facility will be determined during the PFSA. Such a requirement will be based on the type of traffic normally handled by the port facility and the potential for the port facility to handle specific traffic types or cargoes on an occasional basis. Such traffic types / cargoes include cruise ships, military vessels and high consequence dangerous goods (as listed in Annex J).

Where it is not possible to determine in advance the precise location of these vessels and cargoes, several alternative TRAs may be agreed. However, all designations must be detailed in the PFSP and therefore approved by the DA.

Prior to bringing a TRA into use, a thorough security sweep of the area must be carried out. The sweep procedure must cover the entire area with the purpose of ensuring that no persons or suspicious items are present. Written instructions covering the sweep procedure should be produced and all participating personnel provided with a copy.

TRAs must be secured and monitored, and search regimes implemented, in line with the requirements for permanent Restricted Areas. Where temporary fencing is used, this must be open weld mesh fencing that is a minimum of two Metres (2m) high with concrete feet and panels that are bolted together. The gap underneath the fencing must be small enough to deny access.

Port facilities are required to ensure that access to Temporary Restricted Areas is not facilitated by the proximity of vehicles or any other item that could be used as a climbing aid to help circumvent the fence. The requirement to maintain this "clear zone" remains constant irrespective of the prevailing Security Level.

Part 3: Designated Controlled Buildings

The requirement to designate Controlled Buildings within a port facility will be determined during the PFSA. Any building within the port facility may be designated as a Controlled Building. Although designation will vary depending on the specific assets, infrastructure and vulnerabilities of the port facility, the following buildings will generally be classed as Controlled Buildings:

- port management office
- other locations where security sensitive information is held
- vessel traffic management system control rooms
- areas where security and surveillance equipment is stored or located

The above list is purely indicative, and buildings will be considered on a case by case basis. Alternatively, strong rooms or controlled floors can be created whereby access to the wider building is unrestricted, and security measures are only placed on the room or floor containing either security sensitive or port operation equipment or information. This will be an effective solution where designation of the whole building may result in operational difficulties. This issue will continue to be determined on a case by case basis during the PFSA programme. There will be no designation of Temporary Controlled Buildings.

Controlled Buildings are required to have external CCTV coverage, area lighting and checks by security patrols, as outlined for Restricted Areas. If a controlled room / floor has been designated instead of a Controlled Building, then CCTV must be used to monitor the entrances / exits of the room or floor. However, buildings will obviously not require fencing. All windows and doors must be secured by locks when the building is not in use.

It is recommended that doors are fitted with five lever mortice deadlocks or mortice rim deadlocks and that guards / receptionists or automatic access control systems, such as keypad activated locks or proximity card turnstiles, are used at all access points when the building is in use. Intruder Detection Systems (IDS) (burglar alarms) are also recommended and technical advice on such systems can be obtained from the DA. Openings in walls forming part of the perimeter of a Restricted Area, e.g. doors, windows and loading bays must always either be secured or be controlled .

Port facilities are required to ensure that access to Controlled Buildings/Floors/Rooms is not facilitated by the proximity of vehicles or any other item that could be used as a climbing aid to help breach the integrity of the building. The requirement to maintain this “clear zone” remains constant irrespective of the prevailing Security Level.

At Security Level 2 consideration should be given to increasing the size of the “clear zone”. Although the DA understands the constraints resulting from the size and shape of the port facility every effort should be made to increase the “clear zone” for example, by restricting vehicular access as outlined above. The "clear zone" is also intended to provide a clear line of sight to security staff and minimise the damage to the controlled building.

Part 4: Schematics

Port facilities are required to include in the PFSP a schematic(s) of the port facility showing the following:

- Proposed Restricted Areas (RA);
- Proposed Temporary Restricted Areas (TRA);
- Proposed Controlled Buildings (CB); and
- Proposed Access points to all RAs, TRAs and CBs.

These proposed areas will be designated by the approval of the plan.

Schematics should be to a suitable scale to enable all boundaries to be clearly identified but should be no less than 1:1250.

Part 5: Securing Restricted Areas

The perimeter of Restricted Areas must be secured using fencing, gates and/or walls. Perimeter fencing will form a barrier to intruders and delineate the boundary of the Restricted Area. The level of protection afforded by a fence depends on a number of factors including its height, construction and the material used. The minimum height for the fence line should be 8 feet high with 2 feet of 3-strand barbed wire, 45 degrees from vertical, angled away from the facility. If chain-link fencing is used, it must be concreted into the ground at its base. RA's located within a facility fenced to these standards need not have a secondary fence to this standard, but must have appropriate signage and all access points must be controlled.

Port facilities should take particular care to ensure that there are no weak points in the perimeter, for example where gates form part of the fence line or where fence meets wall.

Port facilities must also ensure that all adjoining properties of a Restricted Area fence line / wall, and the area surrounding Controlled Buildings, are clear of all objects that might aid infiltration to or withdrawal from the area or building, or might be used to conceal movement.

In keeping with security best practices, the perimeter fence **must** be kept clear of all obstructions within 3.0480m ten (10) feet. Hence all containers, debris, buildings, or anything that can be used to facilitate unauthorised entry to the port must be placed away from the perimeter fence.

Part 6: Pass Systems – *Part B 16.12- 16.13*

Port facilities are required to have pass systems for all those requiring access to Restricted Areas and Controlled Buildings and, wherever possible, for those requiring access to the port facility. The primary purpose of a pass system is to aid identification and control access within a Restricted Area / Controlled Building. Where a port facility is co-located with other port facilities, the PFSO may wish to co-ordinate pass systems with those of other port facilities.

Port facility pass systems must include full passes, temporary passes and day passes for both persons and vehicles. Details of the types of pass, and the minimum requirements for passes, are given below.

Full Passes

An identity document produced either automatically or manually, must be issued to all members of staff employed at the port facility that require regular, authorised and unescorted access to a Restricted Area or Controlled Building.

Before a full pass is issued, the PFSO must be satisfied that adequate background checks have been carried out. This must include checks of two forms of identification, including a passport wherever possible, and a criminal record check.

All full passes must incorporate the following features in their design:

- A recent photograph and full name of the holder.
- A pass-specific serial number.
- A readily identifiable, port/port facility specific design or logo.
- Colour or shading to enable full passes to be easily distinguished from other passes.
- Expiry Date.

It is also recommended that the following details are included on the reverse of the pass:

- A return address in case of loss and/or instructions to hand the pass in to the nearest police station.
- Date of issue.

All full passes must be sufficient to allow easy visual confirmation by a security guard or supervisor that the person presenting the pass is that pictured on the pass.

Employers of port staff issued with full passes must verify employment and confirm that loss, misuse or failure to display the pass by the employee will be subject to an investigation and possible disciplinary action under that employee's terms of employment.

Full passes may be issued to ships' crew where individuals are regular members of crew on board ships providing regular services to or from the port facility, subject to the requirements outlined above. In addition, the crew member's employer must verify employment and confirm that loss, misuse or failure to display the pass by the crew member will be subject to an investigation and possible disciplinary action under that employee's terms of employment. If full passes are not issued to ships’ crews, the ship must provide suitable ID cards for their staff.

Temporary Passes

A temporary pass must be issued to all contractors, consultants and regular trade persons who are employed for **specific** periods of time or who may require occasional, authorised and unescorted access to a Restricted Zone or Controlled Building. Temporary passes must incorporate the same features as full passes, but are not required to include a photograph of the pass holder.

Before a temporary pass is issued, all contractors, consultants and regular trade persons must present at least one valid form of identification (preferably a passport or drivers licence) and provide evidence/a valid reason for requiring access to the area or building.

At Security Level 3, temporary passes may be revoked and persons may be required to obtain day passes. Access by non-essential persons should be denied. Those granted access must be escorted for the duration of their time at the port facility.

Day Passes

A day pass must be issued to all visitors and occasional trades persons requiring access to a Restricted Area or Controlled Building. Day passes must incorporate the same features as full passes but are not required to include a photograph of the pass holder.

Before a day pass is issued, visitors / trades persons must present at least one valid form of photo identification (preferably a passport or drivers licence) and provide a valid reason for requiring access to the area or building.

At Security Level 3, access by all non-essential persons should be denied. Those given access must be escorted throughout the duration of their time at the port facility.

Vehicle Passes

Full, temporary or day vehicle passes (as appropriate) must be issued to all persons requiring access to a Restricted Area by vehicle or wishing to park within the port facility. All vehicle passes must include the following details:

- Vehicle Registration
- Make and model of vehicle
- A pass-specific serial number.
- A readily identifiable, port/ port facility specific design or logo.
- Colour or shading to enable full passes to be easily distinguished from other passes.
- Expiry Date.

Before a vehicle pass is issued, the equivalent identification requirements for full, temporary and day passes outlined above must be met.

When an individual requires access in more than one vehicle, a full pass may, at the discretion of the PFSO, include details of more than one vehicle.

Wherever possible, vehicle passes should be specific to individual car parks or parking areas within the port facility and/or specific to individual Restricted Areas where there is more than one within the port facility.

Alternatively, an approved roster system can be used whereby approved drivers are listed on a record held by security staff at each facility. The vehicles of persons not on this list will be denied entry to the facility. The PFSO is responsible for management of the roster.

Automated Pass Systems

Passes may incorporate electronic recognition capabilities to provide for automated access control systems. Electronic pass systems allow users to access Restricted Areas or Controlled Buildings by inserting or swiping uniquely coded access cards through a reader, which may, for additional security, incorporate a keypad requiring an access code. The most commonly used electronic cards include magnetic strip cards and proximity reader cards.

It is considered necessary for all passes to have expiry dates, whether manual or automated. This will assist pass validity checks, such as those to be undertaken at Security Level 2 (when automated systems at access points must be checked periodically by security patrols to ensure that all passes are valid). It will also ensure that, for example, during a power failure when automated systems may be out of action, security guards/officers can still ascertain the validity of passes.

Record Maintenance

PFSOs have overall responsibility for maintaining a comprehensive record of passes issued for access to a Restricted Area or Controlled Building (or the port facility as a whole). These records must include the following details:

For all passes:

- name of pass holder
- date of issue
- date of expiry
- areas to which access is required
- name of person issuing pass

For full passes:

pass holder's appointment or position
whether a new or replacement pass
reason for replacement (if applicable)

- vehicle registration
- make and model of vehicle

For temporary and day passes:

- company or organisation
- reason for visit and area or person to be visited
- time in / date of issue
- time out / date of expiry
- vehicle registration
- make and model of vehicle

All pass issue records are subject to audit by DA security inspectors and must be retained for a minimum of 12 months.

All persons issued with a pass, whether full, temporary or day, must be made aware of the requirement to return the pass to the PFSO or relevant authorised person when employment is discontinued or upon exiting the port facility.

Pass Wearing and Durability

Personnel in possession of passes must display them openly and visibly above waist height whilst present within the port facility. PFSOs should consider the safety implications of this requirement and should consider, for example, acquiring high visibility jackets and/or overalls with chest mounted weatherproof plastic holders.

All passes must be capable of maintaining their integrity in all weather conditions. Sticky labels are not sufficient as passes.

Personnel in possession of vehicle passes must ensure that they are displayed openly and visibly in the vehicle whilst it is present within the port facility.

Loss, misuse and failure to display a pass should be the subject of an enquiry/disciplinary procedure under that employee's terms of employment.

If a person found to be in contravention of the appropriate pass requirements is not an employee of the port facility operator, that person should either be refused permission to enter the RA or controlled building or be asked to leave the port facility. In any event the person should be informed that future access would be denied unless the pass requirements are met and the relevant employer informed of the contravention. Wherever possible, contracts with companies whose employees require regular access to the port facility should require their employees to adhere to the necessary security requirements. Port operators should inform the relevant employer if the requirement to display a pass is not met and they should be asked to speak to the employee in question.

Authorised Government Officials

The following Government officials are not subject to the pass requirements outlined above when on official business.

- Health Inspectors
- Safety Inspectors
- Police
- Customs officials
- Immigration
- Maritime Authority of Jamaica (MAJ)

However, such persons must be able to provide official identification and/or authorisation documents before access is granted and must display an official pass (or a port facility pass) openly and visibly whilst present within the port facility. Details of official identification documents as a reference for use by security staff can be obtained from the relevant authorities / organisations.

Part 7: Access Control- *Part B 16.10-16.11*

To ensure effective access control, access points must be kept to a minimum. This ensures best practice in the allocation of manpower resources and effective control of both vehicles and persons. Although it is recognised that effective operations in many port facilities will require numerous access points to Restricted Areas, port facilities must consider whether access points that are used only infrequently can be permanently closed. Where closure is possible, the measures used must ensure a level of protection for the Restricted Area that is at least as effective as that provided by fencing and other access control systems.

All access points must be capable of being secured when not in use to a level that is at least as effective as the fencing used to secure the Restricted Area.

At Security Levels 2 and 3, port facilities must consider what additional access points could be closed and secured during the period for which the heightened Security Level prevails.

Access Point Control

Access points may be controlled either by deploying security guards or using suitable access control systems. These systems may be automated, for example using a swipe-card pass system or proximity reader, or manually operated, for example using keypads or locks. The primary purpose of access control is to ensure that only authorised persons gain access to Restricted Areas. It is therefore essential that inspection / verification of passes occurs at all manned access points and that all passes, keys, passwords, etc, used in the operation of access control systems are closely regulated.

At Security Levels 2 and 3, guards at manned access points should enhance scrutiny of all passes and should question those requiring access to confirm the reason for access.

At Security Level 3, access will be controlled by the on-site Incident Commander.

At Security Level 2, unmanned/automated access points should be subjected to random checks by security patrols to ensure continued operation of access systems and to undertake random pass checks of those requiring access. At Security Level 3 unmanned access points should be permanently manned or closed and secured.

Manned access points must have suitable control posts to ensure continued, effective access control in all weather conditions and to ensure the security of any pass issuing systems located at access points. When installing control posts advice should be sought from the DA on a case by case basis.

It is recommended that vehicle access points have 'lock gate' access systems. These systems have two control barriers, such as vehicle drop arm/swinging arm barriers (with skirts), allowing effective vehicle control. These should be employed to control and regulate the flow of traffic into and out of the Restricted Area.

Vehicle access control is vital at PAX facilities and gates/gatehouses and access control procedures must be robust and efficient. You must ensure that gates are of at least the same standard (height and build quality) as the fence or wall, and are locked closed or controlled at all times.

Procedures for Dealing with Unauthorised Access

Instances of persons seeking to obtain unauthorised access to Restricted Areas, for example by trying to obtain a pass through deception or by breaching the Restricted Area perimeter, should be investigated. The response to such incidents will vary, for example in some cases it may be appropriate to involve the police. The DA is aware that many ports have well-established procedures in place for dealing with such incidents and the PFSP should detail the action that will be taken. Further, specific guidance can be requested from the DA if necessary.

Part 8: Perimeter Intruder Detection Systems (PIDS)

There is no mandatory requirement for port facilities to install Perimeter Intruder Detection Systems (PIDS) but some may already have these systems in place or may choose to install them in order to improve detection capabilities and/or upgrade the deterrent effect of existing fencing.

Part 9: Checks and Searching - *Part B 16.18*

Checks, searching and screening provide both deterrence and active detection of articles, goods or substances that could be used to cause a security incident. Searching of people, baggage, vehicles, ships' stores, cargo and freight is required at passenger port facilities at all Security Levels.

The required search percentage at each Security Level will depend on the prevailing levels of threat and risk and may vary within a set range, as shown in Annex A. The use of percentage ranges allows more flexibility and will ensure that the DA / ports facilities are able to respond to small-scale changes in threat or risk without necessarily requiring large-scale changes in security measures on the ground.

The prevailing search percentages will be set by the DA and notified to port facilities by way of a separate instruction (a Security Standards Matrix) which will be re-issued whenever percentages change. An example of the Security Standards Matrix can be found at Annex G. Percentages will be changed only based on changing threat and risk information and percentages will be set at intervals of no less than 5%.

Search requirements are listed at Annex A

Depending on the nature of the threat or risk information, search percentages may be changed for all port facilities and all search types (i.e. passenger, vehicle, cargo, ship's stores, etc).

Search percentages for people, baggage and vehicles require a certain percentage of total throughput to be searched. For example, if the search percentage for persons is 30% and 100 people require access to a Restricted Area in the course of a day, 30 of those persons must be searched.

Port facilities are not required to purchase or use screening equipment such as X-ray or Archway Metal Detectors. However, port facilities are strongly advised that such equipment should be used wherever possible to improve both the efficiency and effectiveness of searching. Screening equipment may also assist port facilities to meet higher search percentages at Security Levels 2 and 3 and port facilities may wish to hire equipment for the duration of the increased security requirements.

The checks and searches outlined below are for counter terrorism purposes and are to be carried out principally to deter the carriage of prohibited items and to detect the presence of firearms and/or explosives. A list of articles considered as dangerous and that should therefore be prohibited from Restricted Areas, Controlled Buildings and ships, unless there is a valid lawful reason, can be found at Annex H. The list also provides examples of property that passengers should be allowed to retain unless there is reason to suspect the item may be used to commit an act of violence.

Searching of Staff, Visitors, Ship's Crew and their Vehicles –
All staff, visitors, ships' crew and their vehicles must be liable to search upon entry into a Restricted Area. Searching must be conducted in accordance with the requirements outlined below for person and vehicle searching. Security patrol guards / officers may be exempt from searching whilst conducting official security patrols.

A search of a vehicle, or part therein, requires the driver to witness an in-depth search of the area of the vehicle together with any items in that area. Checks of vehicles are visual inspections only and may lead to a search if suspect items are noticed by security staff.

All vehicles entering the port facilities must have at least one area within them visually checked by security staff.

The searching of cars and other vehicles should be varied to include basic questioning of the driver and, where necessary, other passengers. It must also include at least two of the seven checks set out below, selected on a random basis.

- **Boot interior:** check content of bags and boxes and check spare wheel space.
- **Vehicle interior:** check under seats, inside glove boxes, in door storage spaces and behind sun visors.

- **Engine compartment:** check for concealed items.
- **Under vehicle:** check for concealed items attached to underside of vehicle, including the wheel arches.
- **Roof box:** check interior and search content of bags and any other stored items.
- **Body search:** search driver and passengers.
- **Trailers:** check interior of trailers, such as those carrying tents, horse boxes, yachts or other pleasure craft. Contents may need to be removed for further searching.

All persons undertaking searching must be trained in search techniques. Search teams must include officers trained in body search techniques to undertake searches of drivers and passengers. Although this will mean that a trained male searcher needs to be in place throughout the operating period in order to carry out these checks, it does **not** mean that a female officer must also be in place. It is acceptable for procedures to be developed locally which enable a trained female searcher to be called upon when necessary.

At Security Levels 2 and 3 the percentage of searching required will increase. At Security Level 2 searching of vehicles must include at least four of the eight checks set out above. At Security Level 3 searching of vehicles should include all eight checks.

All search equipment must be in full working order. For hand held equipment such as HHMD or under car mirrors, spare batteries should be kept to hand and broken mirrors replaced as soon as possible. Search teams should be equipped with torches and mirrors to assist with under vehicle / wheel arch checks.

Body Searching of visitors, staff, ships' crew etc

All persons must be liable to search upon entry into a Restricted Area.

All persons undertaking searching must be trained in search techniques including body search. Additional tasking of searchers to cover matters such as access control and boarding card checks should be avoided as this invariably means that the full requirements of the search duties are not met.

Searching of persons must be varied so that no particular pattern is discernible to anyone observing the procedure. The procedure should include basic questioning, bag searching and body searching.

Port facilities that operate X-ray equipment, trace and/or vapour detection equipment must ensure that sufficient numbers of suitably trained staff are in place to operate the equipment effectively.

Some hands-on body searching must take place during searching irrespective of a port facility's use of screening equipment.

All search equipment must be in full working order and such machines should be properly maintained and calibrated as per manufacturer's guidance. For hand held equipment, such as *'hand held metal detector'* (HHMD), spare batteries should be kept to hand. Calibration should be set in accordance with the manufacturer's instructions to enable the equipment to pass any test carried out by the DA.

At Security Levels 2 and 3 the percentage of searching required will increase but the methods of searching will not change.

Container Ro-Ro Freight Screening

All freight must be liable to search upon entry into a Restricted Area.

The screening of freight, either accompanied or unaccompanied, is an essential part of the overall search process. Selection for screening must take place on a random basis and must be varied so that no particular pattern is discernible to anyone observing the procedure.

Screening procedures must include examination of relevant paperwork and questioning of drivers to authenticate the load and journey undertaken. Authentication of journey and load details helps to establish a baseline of deterrent security. In this respect all freight vehicles should be subject, on a random basis, to checking as they enter a Restricted Area.

Screening must include checks of the exterior of the vehicle, container and/or trailer for signs of tampering, such as broken seals. Where a container / trailer is reported to be empty, and no intact seal is present, a visual check should be made of the interior. Operators are not expected to break seals in order to carry out checks or to open containers / trailers if the driver cannot verify that it is empty.

It is acknowledged that paperwork may not always be available and port facility operators are asked to encourage all regular haulage companies, shipping companies, etc. to provide an alternative means of assisting verification of the load content and to check that the consignment is expected. When paperwork is not available a vehicle need not be turned away automatically at Security Levels 1 and 2. Drivers should be questioned further and in more detail about the load, for example its origin, destination and content.

Each of the criterion is an indicator and the greater the number of criteria matched the greater the police interest is likely to be. However, there must also be consideration given to what is normal traffic for the port. Some of the criteria may in fact be regarded as routine, such as cash payments, and will not necessarily give cause for concern. This can only be established locally and will be subject to change.

- Cash payment
- Non-account/contract customers
- Driver having no knowledge of load
- Inconsistency between weight of load and documentation details
- An older and possibly defective vehicle
- An unliveried vehicle
- A hired vehicle

- A trailer lacking identification marks
- A vehicle with unclear or dirty number plates
- A driver reluctant to answer questions

To ensure this identification process can be applied effectively, port facility operators should discuss and develop procedures with the assistance of local customs officers at ports.

If a freight load is identified as being a cause for concern, it will be necessary to have a set of agreed procedures in place detailing the follow up action to be taken. For example, this may involve moving the vehicle to a designated location within the port facility/port area. This will need to have been agreed in advance with the relevant agencies. Operators should therefore ensure that their port/terminal contingency plans take account of these issues.

At Security Levels 1, 2 and 3 all containers departing Jamaican ports will be screened and port facilities are required to undertake searches of the vehicles' cabs and drivers, as outlined below. Cab searching applies to any vehicle requiring access to a Restricted Area, whether the load is travelling accompanied or unaccompanied. This is to ensure the integrity of the Restricted Area.

Searching procedures must include checks of the exterior and interior of the vehicle cab. The container and/or trailer must be visually examined for signs of tampering, such as broken seals. Checks should include basic questioning of the driver and, where necessary, other passengers. When such searches are conducted they must also include at least two of the six area checks set out below, selected on a random basis.

Cab interior: under seats and behind sun visors and the various storage areas within the cab including all overhead boxes, door stowage areas and any sleeping area at the rear of the cab. This check must also include searching of the cab's occupants (male and female) and their baggage. Although this will mean that a trained male searcher needs to be in place throughout the operating period to carry out these checks, it does **not** mean that a female officer must also be in place. As many lorry cab occupants are male, it is acceptable for procedures to be developed locally which enable a trained female searcher to be called upon when necessary.

Cab searches are for counter terrorism purposes and are to be carried out principally to discover the presence of firearms and/or explosives. If, during the searches of lorry cabs, any prohibited items are found, the driver(s)/occupants of the cab should not be allowed to travel with the items.

Cab exterior: engine compartment check for concealed items;

Under vehicle: check for concealed items attached to underside of vehicle, including wheel arches (mirrors and torches should be used);

Container/Trailer exterior: check for signs of tampering and any unusual features, for example deeper than normal trailer beds or signs of unusual welding;

Container Seals: check integrity of seal if used;

Internal check of unsealed empty container: must be subject to search during the operational time that vehicles are subject to checking;

Note: It is acknowledged that many cabs involved in Ro-Ro operations will require access to a Restricted Area but will not board a ship. However, in order to ensure the integrity of any Restricted Area, all cabs entering such areas must be liable to search.

Unaccompanied Loads- Part B 16.30 -16.37

Any Ro-Ro freight loads travelling unaccompanied, i.e. drop-trailers without a driver, should be subject to a visual check of the exterior and seals (if used) for any signs of having been tampered with.

Empty Containers

Where a container / trailer is reported to be empty, and no intact seal is present, a visual check should be made of the interior. Operators are not expected to break seals in order to carry out checks or to open containers / trailers if the driver cannot verify that it is empty. However, the container will be subject to non intrusive screening at the port, where such a system exists, and subject to the findings of this screening, may be identified to be opened and searched.

Sealed Containers

Health and Safety and insurance issues relating to the opening of containers means that ports will not be required to open packed containers and will not, therefore, be required to break customs or shipping line seals. Although ports will be required to check some empty containers we do not wish for ports to reduce the effectiveness of existing tracking and audit procedures, which we encourage. Ports will not be asked to check the interior of empty containers if they have been sealed and the seal is intact. Such containers would remain liable to search by Customs officers on an intelligence led basis and we feel that this is a sufficient preventative regime at the present time. However, where applicable, the container will be subject to non-intrusive screening at the port and subject to the findings of this screening, may be identified to be opened and searched.

Searching of Ships' Stores - Part B 16.38-16.43

All delivery vehicles carrying ships' stores must be liable to search upon entry into a Restricted Area. Such searches could include manifest reconciliation, checking that the delivery is expected and/or an exterior or cab search of the vehicle.

Processing of ships' stores must include the checking of delivery notes to ensure the supply corresponds with the paperwork and is from the expected or known supplier and is expected by the ship. Details of the driver and vehicle registration number should, wherever possible, be checked against supplier details. Visual inspections to check the integrity of the packaging and to check the supplies for signs of tampering will be carried out by the ships' crew.

Delivery vehicles must be searched in line with the overall vehicle-searching regime as outlined earlier in this Chapter.

All stores will be subject to either intrusive or non-intrusive screening at the port.

Search Statistics

Search statistics for all forms of searching must be kept and may be subject to inspection by DA inspectors. Statistics must be kept in a format that allows inspectors to discern the number of passengers, freight and stores were searched and the type of search undertaken, i.e. body, baggage, vehicle interior, vehicle underside, etc. An example log sheet is shown at Annex I.

Search Equipment

Apart from improving the deterrent effect of the security system, measures at the higher security levels are intended to enhance the detection capability of the searching arrangements. It is therefore recommended that equipment such as trace detectors be used, at higher Security Levels, when port facilities may wish to hire, lease or borrow appropriate equipment.

Technical advice on appropriate standards and use of search equipment can be obtained on a case by case basis from the DA.

International Initiatives

Jamaica has also signed up the US Container Security Initiative (CSI) and US Customs officials, based in Kingston, are working closely with local Customs officers.

CSI is an intelligence led operation, which targets suspect containers. US officials have no executive powers in Jamaica and therefore work closely with their local counterparts so that suspect containers can be intercepted, opened and subject to search. Although in operational terms this is a relatively new concept the early signs have been extremely encouraging.

Part 10: Monitoring – *Part B 16.49- 16.54*

Port facilities are required to monitor Restricted Areas and Controlled Buildings at all Security Levels using a combination of CCTV and security patrols, combined with adequate lighting. Port facilities are also required to monitor seaward approaches at Security Levels 2 and 3.

Lighting – Part B 16.49.1

Port facilities are required to use perimeter lighting to illuminate the perimeter of Restricted Areas and area lighting to illuminate the immediate area around Controlled Buildings. The primary benefits of security lighting are:

- to act as a deterrent to unauthorised intruders;
- to assist in visual observation of strategic areas and the perimeter; and
- to support other detection methods such as CCTV.

The minimum requirement for lighting levels is 3-LUX operational (5-LUX on commissioning) for perimeter lighting and 3-LUX over the defined area for area lighting.

When installing lighting systems, port facilities should consider, in particular:

- whether the lighting will cause a hazard, particularly to shipping (lighting should be configured in such a way as to avoid impairing the night vision of those trying to conduct berthing manoeuvres);
- how to minimise the potential for the lighting to cause distress to local interests;
- the cost effectiveness and reliability of the system; and
- compatibility with CCTV systems (colour CCTV is ineffective without appropriate lighting).

Perimeter Lighting

Perimeter lighting provides a well-lit area in the form of a strip around, but usually clear of the protected area. To be effective, an intruder must have to pass through this well-lit area to reach the protection area.

The lighting columns should be located so that the ground immediately outside the fence is adequately illuminated but the inside face of the fence is not, thus allowing guards clear vision through the fabric of the fence. This can be achieved by using an outreach arm from the light post, placing the luminaire above and slightly beyond the fence line.

The lighting columns should be positioned at least 2m inside the fence line. This will prevent intruders using them as climbing aids, to defeat any Perimeter Intruder Detection Systems (PIDS) or physical barrier. They should also be spaced at 3 to 4 times their mounting height.

The variation in horizontal illumination level (uniformity), within the area to be lit should not exceed 3:1 (average to minimum) when all lamps are lit. When CCTV is in use, the ratio should be kept below 10:1 with one lamp out.

A minimum horizontal illumination level of 3-LUX operational (5-LUX on commissioning) should be the design criteria. An allowance should be added to allow for deterioration of lamp output as the lamp ages and dirt builds up on the luminaire, together with possible reductions in supply voltage.

Area Lighting

This form of lighting is generally used to illuminate the area around protected buildings. Full use of existing lighting should be made but if this is inadequate in some areas supplementary lighting may be required. Where existing amenity lighting levels are high it may be necessary to provide higher area lighting levels than would otherwise be needed to avoid excessive variations in light levels.

The minimum illumination should exceed 3-LUX over the defined area, with a uniformity of 3:1 average to minimum.

Closed Circuit Television (CCTV) Systems

CCTV Systems are not a requirement of the ISPS Code. However, if a port chooses to use these systems then they must achieve the following:
CCTV systems must be capable of covering the perimeter of all Restricted Areas and the exterior and entrances / exits of all Controlled Buildings. If a controlled room / floor has been designated instead of a Controlled Building, then CCTV must be used to monitor the entrances / exits of the room or floor. CCTV systems must also be capable of monitoring seaward approaches at Security Levels 2 and 3, for example by the installation of a Pan-Tilt-Zoom (PTZ) camera(s). Coverage of seaward approaches need not be continuous, and cameras may be programmed to switch between views on a regular basis.

Before any system is agreed, a site survey should take place under controlled conditions during which the area(s) to be monitored should be clearly identified and the operational requirements determined.

At Security Level 1 the CCTV system must be recorded and records held for a minimum of ninety (90) days. Such recordings may be kept in either analogue format (e.g. videotape) or digital format (e.g. CD and / or PC hard drive).

At Security Level 2, the CCTV system must be monitored. Clear and concise instructions should be written for security officers or others charged with monitoring CCTV from a control room or elsewhere. They should take into consideration manpower and health and safety requirements for time spent in front of monitors or banks of monitors.

Lighting for CCTV

CCTV cameras are very similar to the human eye in that they detect only the reflected light from a scene and some detect colours better than others do. Therefore, the choice of lighting for use with a CCTV system can be critical. Low-pressure sodium lamps are currently the most cost effective available, but the light emitted is monochromatic - single colour - in this case yellow. So, the use of a colour camera lit by low-pressure sodium would be pointless. However, a black and white camera, working with low-pressure sodium lamps would be acceptable.

The situating of cameras and/or lights must be considered very carefully. Account must be taken of shiny surfaces, topography, foliage, weather and the interaction of these occurrences on the whole security system.

Part 11: Security Patrols – Part B 16.49.2

Security patrols are required to ensure the integrity of Restricted Areas and Controlled Buildings and to monitor activity within the port facility. At Security

Level 1 patrols must be undertaken at hourly intervals. At Security Level 2 patrols must be undertaken at 30-minute intervals and at Security Level 3 patrols must be continuous.

Patrols must cover all Restricted Area and Controlled Building perimeters and access points. Although patrol routes and intervals should be varied so that no particular pattern is discernible to anyone observing the procedure, it will be necessary to produce clearly written instructions for patrol guards / officers detailing patrol requirements.

Patrols should cover at least:

- perimeter fencing
- access control points
- lighting
- CCTV blind spots
- Controlled Building/floor/room access points (doors and windows)
- quayside and ship gangways
- vehicle parking areas
- any other critical targets identified in the PFSA

In conducting these patrols, consideration should be given to the following:

- the integrity of the fence line;
- whether all access points are secured or controlled;
- whether lighting is in full working order;
- whether Controlled Building/floor/room access points are secured or controlled; and
- whether vehicles are displaying valid passes.

Staff conducting patrols must be suitably equipped to enable them to detect and respond effectively to any discovered deficiencies.

Equipment must include:

- Torches
- Communication
- Notebook and Pen
- Patrol Whistle (Foot patrols)

It is important that procedures are in place to enable patrol staff to call upon support if required and that they be briefed on the expectations of their role. Patrol staff are not expected to place themselves in unnecessary danger, for example there is no expectation that they would apprehend an intruder, in such cases police back up should be requested.

Part 12: Vehicle Parking

All vehicles parking within the port facility must be controlled at Security Level 1 using a vehicle access system, as outlined in Chapter 5 Part 6, and vehicle passes should be checked regularly by security patrols. All vehicles parked within a Restricted Area must be subject to checking by security patrols.

At Security Level 2 vehicle parking must be restricted as much as possible, and attention should be paid to parking areas adjacent to Restricted Areas, Controlled Buildings and the Ship/Port interface, for example by restricting the ability to park in these areas to full pass holders only. Wherever possible alternative parking should be found outside the port facility and/or away from Restricted Areas, Controlled Buildings and the Ship/Port interface.

At Security Level 3 all non-essential parking must be prohibited within the port facility and parking must be restricted to key operational staff only.

Part 13: Seaward Protection

At Security Level 1 – Ad hoc patrols in the area.
At Security Level 2 – Permanent presence in the harbour area
At Security Level 3 – As Security level 2

CHAPTER 6: SPECIAL REQUIREMENTS

CHAPTER 7: DEFINITIONS AND GLOSSARY OF TERMS

Port Facility Security Assessment (PFSA)
The process by which DA Inspectors identify key assets within a port facility, assess the threats to these assets and identify security measures that can be implemented to reduce the vulnerability of these assets.

Port Facility Security Officer (PFSO)
The person designated as responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan and for liaison with the Ship Security Officers and Company Security Officers.

Port Facility Security Plan (PFSP)
A plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ships' stores within the port facility from the threat of a security incident.

Port Facility Security Instructions (PFSI)
Information provided by DA to port facilities giving details of legal requirements and guidance for implementing the necessary security measures at each Security Level.

Port Facility
A location, as determined by the Jamaican Government, where interactions occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provision of port services to or from the ship. It includes areas such as anchorages, waiting berths and approaches from seaward.

Restricted Area
An area, which may cover an entire port facility or part of one, identified during the PFSA process as requiring specific protective security measures, including access control.

Controlled Building
A building identified during the PFSA process as requiring specific protective security measures because of the sensitive equipment and / or information contained within it – can be a room or floor within a building.

Ship/Port Interface
The interaction that occurs when a ship is directly affected by actions involving the movement of people, cargo, stores or other goods or the application of port services to or from the ship.

PAJ
Port Authority of Jamaica

CHAPTER 8: SOURCES OF ADDITIONAL INFORMATION

General and Specific Advice and Information from the DA

PAJ MARITIME

Telephone: 922-0290/9

Technical Advice on Security Equipment and Standards

PAJ (as above)

Copies of International, European and JAMAICA Legal Documents

Copies of the ISPS Code can be purchased from the IMO.

International Maritime Organization
4 Albert Embankment
London SE1 7SR
E-mail: publications-sales@imo.org
Tel: 020 7735 7611
Fax: 020 7587 3241
Web site: www.imo.org (for online purchases)

SECURITY STANDARDS QUICK REFERENCE: PROTECTION CATEGORY CRR ANNEX A

	SECURITY MEASURE	SL1	SL2	SL3	OVERVIEW OF REQUIREMENTS
	PFSO	✓	✓	✓	Appointed, vetted, trained, approved
	PFSP	✓	✓	✓	Prepared using PFSP template in combination with PFSI and PFSA
	Contingency Plans	✓	✓	✓	Submitted as part of PFSP
MANAGEMENT OF SECURITY	**Port Security Committee**	✓	✓	✓	Meet no less than 4 times per year, chair to be agreed during PFSA, all stakeholder to be involved, can combine with other committees
	Security Level Changes	✓	✓	✓	Informed by PAJ by phone effected within 24hrs,
	Security Training	✓	✓	✓	PFSO approved course, security staff- sec training, other personnel - awareness training
	Security Duties	✓	✓	✓	Staff must be clear about duties and able to carry them out
	Drills and Exercises	✓	✓	✓	Drills (e.g. evacuation, bomb threat) every 3 months, exercises (large-scale) annually
	Security Vetting	✓	✓	✓	PFSO and Deputies must be cleared, no other vetting, background checks for full passes
	PFSP review, amendment and audit	✓	✓	✓	PFSO review and amend if port changes, incident occurs, deficiencies identified, ownership/control changes, internal audit at least annually
	Security Incident Reporting	✓	✓	✓	Internal reporting system for staff and others present in port, system for reporting to PAJ and other agencies
	Evacuation Procedures	✓	✓	✓	
	Information Security	✓	✓	✓	" " - lock away, need to know, PCs - passwords (change regularly)
	Dangerous Goods	✓	✓	✓	
	Equipment Maintenance	✓	✓	✓	Regular maintenance checks as per manufacturers recommendations, faults reported and repaired, back-up systems / procedures required
	Ship-port facility communication links	✓	✓	✓	Procedures for communicating with ships, back-up systems are required
	Ship Security Alert	✓	✓	✓	Policy under development
	Declaration of Security	✓	✓	✓	For interface with non-SOLAS ships, ships or ports at SL3, ship higher SL than port, after security incident, if PAJ request one
	Response Agencies	✓	✓	✓	Keep up to date contact details

ACCESS CONTROL	**Pass Systems**	✓	✓	✓	Full, temporary and day passes for people and vehicles, maintain records, wear visibly
	Access Control	✓	✓	✓	Minimum number of access points, reduce access points at SL2 and again at SL3 (if possible), access points manned, locked or pass controlled barriers
	PIDS				Not mandated, but may be useful under certain circumstances

AREAS	**Areas**	✓	✓	✓	Freight storage areas, utility installations, essential telecomms systems, DG storage
	Temporary Areas	✓	✓	✓	If occasional use of berth outside permanent RA for passenger, military, DG shipment
	Controlled Buildings	✓	✓	✓	Port management office, security sensitive info storage, VTS control rooms, security office
	Schematics	✓	✓	✓	Map / plan no less than 1:1250
	Securing Areas	✓	✓	✓	

SEARCHING	**Cargo / Freight* by operating time**	100%	100%	100%	SL1-3 All local origination containers, whether empty or full are screened prior to departure
	Ship's Stores by % throughput	100%	100%	100%	SL1-3: All Ships stores are screened upon entry into the port facility
	Full Pass Holders	0-30%	30-100%	100%	SL1: Up to 30% SL2: Up to 100% screening SL3: 100% screening
	All Other Staff	5-35%	35 - 100%	100%	SL1: Up to 35% SL2: Up to 100% screening SL3: 100% screening
	Vehicles	5-30%	30-100%	100%	All vehicles checked upon entry at SL1

* port facility required to check interior of those containers picked for search that are marked on paperwork as empty

ANNEX B: CONSOLIDATED MONTHLY INCIDENT REPORT FORM

MONTH AND YEAR:

PORT FACILITY:

INCIDENT TYPE	DETAILS	ACTION (please include details of any significant follow up action taken by Police or Port, e.g. person detained for police questioning, denied travel, cautioned or prosecuted)
Discovery of Firearms and Ammunition		
Discovery of Weapons other than Firearms (e.g. knives, axes)		
Discovery of explosives, suspected explosives or bomb component parts		
Unauthorised access to Restricted Area		
Bomb Warnings		
Miscellaneous Incidents		

Please send to PAJ

Note: Please also include details of any incidents which require immediate notification (see Annex C)

ANNEX C: INCIDENT REPORT FORM FOR IMMEDIATE REPORTING

To: PAJ	For PAJ use only: Incident No: File ref: Date rec'd: Action/Info:

Telephone (day) Telephone (out of hours) Fax	922 0290

REPORT

From:	Tel:
Date:	Time:

INCIDENT / OCCURRENCE

Date:	Time:
Location:	
Details:	

RECTIFICATION ACTION

Name:

ANNEX D: BOMB THREAT CHECKLIST

- **OBTAIN AS MANY FACTS AS POSSIBLE**
- **SWITCH ON RECORDING SYSTEM IF AVAILABLE**

Wording of the threat

....

....

Questions to Ask
When is the bomb going to explode? ....
Where is it now?...
What does it look like? ....
What kind of bomb is it? ....
What will cause it to explode? ....
Did you place the bomb?..
Why? ....
What is your name? ....
What is your address?..
What is your telephone number?..

Sex of caller: Male □ Female □ **Estimated**: Age □ Nationality ....

Threat Language
Well spoken □ Irrational □ Foul □ Incoherent □
Taped message □ Message read by threat maker □

Callers voice		**Background sounds**	
Calm □	Nasal □	Street noises □	Animal noises □
Angry □	Stutter □	Crockery □	Clear □
Excited □	Lisp □	Static □	Voices □
Slow □	Raspy □	PA System □	Local □
Rapid □	Deep □	Music □	Booth □
Soft □	Gagged □	House noises □	Motor □
Loud □	Clearing throat □	Office machinery □	Factory machinery □
Laughter □	Deep breathing □	Other	
Crying □	Cracking voice □		
Normal □	Disguised □		
Distinct □	Accent □		
Slurred □	Familiar □		

If voice is familiar whom did it sound like?..
"Automatic number reveal" equipment - number shown......................................
Name of person to whom the call was reported ....
Name of person receiving the bomb threat call ....
Dated...
Signed ....

ANNEX E: DECLARATION OF SECURITY FORM

Form of a Declaration of Security between a ship and a port facility[1]

DECLARATION OF SECURITY

Name of Ship:	
Port of Registry:	
IMO Number:	
Name of Port Facility:	

This Declaration of Security is valid from ……………….. until ………………, for the following activities

…………………………………………..
(list the activities with relevant details)

under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility:	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of Part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with relevant approved plan, by	
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		

[1] This form of Declaration of Security is for use between a ship and a port facility. If the Declaration of Security is to cover two ships this model should be appropriately modified.

Delivery of ship’s stores		
Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and Part A of Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at ………………………………………..…….on the ……………………………………

Signed for and on behalf of	
the port facility:	the ship:
(Signature of Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*
Name and title of person who signed	
Name:	Name:
Title :	Title :

Contact Details *(to be completed as appropriate)* *(indicate the telephone numbers or the radio channels or frequencies to be used)*	
for the port facility:	for the ship:
Port Facility	Master
Port Facility Security Officer	Ship Security Officer
	Company
	Company Security Officer

ANNEX F: WORDING FOR RESTRICTED AREA SIGNS

Suggested wording for signs around Restricted Areas:

RESTRICTED AREA

PASSENGERS AND PASS HOLDERS ONLY

ENTRY INTO THIS AREA WITHOUT AUTHORISATION

WILL RENDER YOU LIABLE TO PROSECUTION

Legislation reference

Suggested wording for signs at Restricted Area access and search points:

MARITIME SECURITY

IN THE INTEREST OF PUBLIC SAFETY AND SECURITY

SEARCHING

UNDER THE PROVISIONS OF THE
Legislation reference
YOU MAY BE REQUIRED TO SUBMIT YOURSELF
YOUR BAGGAGE AND YOUR VEHICLE TO SEARCHING
AS A CONDITION OF ENTRY TO THIS RESTRICTED AREA

ANNEX G: EXAMPLE SECURITY STANDARDS MATRIX

SECURITY STANDARDS MATRIX
Protection Category CRR

Security Level = Security Level 1

Required search percentages:

Cargo / Freight* by operating time	100%	100%	100%
Ship's Stores by % throughput	100%	100%	100%
Full Pass Holders	0%	30%	100%
All Other Staff	5%	35%	100%
Vehicles	5%	30%	100%

Note:
Percentages that have increased are shown in bold.
Percentages that have decreased are shown in italics.

ANNEX H: LIST OF PROHIBITED ARTICLES

The following items must not be allowed into Restricted Areas, Controlled Buildings or on-board ship without valid lawful reason.

- **All firearms** (These may only be carried in accordance with company instructions and PAJ requirements.)
- **All ammunition** (This may only be carried in accordance with company instructions and PAJ requirements.)
- **All explosives** including explosive devices, detonators, smoke cartridges, grenades, mines, explosive military stores, imitation explosives, imitation devices, fireworks and flares.
- **Sharp pointed weapons**
- **Flick knives, gravity knives, daggers, lock knives, folding pocket knives** (with a blade over 7cm in length) and **diver's knives** (if not accompanied by other diving/snorkelling equipment and/or a valid diving ID card/licence**)**.
- **Swords, sword sticks and umbrellas containing sword blades**
- **Open razors** such as cut-throat razors.
- **Spears and spearguns**
- **Archery equipment including crossbows and bolts**
- **Knuckle dusters, clubs, coshes and rice flails**
- **Items containing incapacitating substances** such as gas guns, tear gas sprays, mace, phosphorus, acid and other dangerous chemicals that could be used to maim or disable.
- **Inflammable substances, unless carried in limited quantities and in accordance with company instructions** e.g. petrol, methylated spirits, paint thinners, etc.
- **Any other item adapted or intended for use as an offensive weapon**

The following are examples of property which passengers should be allowed to retain unless there is a specific reason for not doing so, or there is reason to suspect that the item may be used to commit an act of violence.

- **Toy guns** that do not have the appearance of a genuine weapon.
- **Catapults**
- **Household cutlery**
- **Camping knives and folding pocket knives** with blades of less than 7cm.
- **Household scissors**
- **Darts**
- **Knitting needles**
- **Sporting bats, pool and snooker cues**
- **Hypodermic syringes**
- **Tradesmans tools**
- **Shreik alarms**
- **Handcuffs**
- **Butane gas canisters**
- **Cosmetics**

ANNEX I: VEHICLE SEARCH STATISTICS

Name of port facility:..
Date:...
Time of sailing: ....
Number of vehicles embarked:...

Please tick (4) appropriate columns following search

Vehicle Type and Registration Number	1	2	3	4	5	6	7	8	Remarks

1: Boot interior
2: Vehicle interior
3: Body searching
4: Caravans
5: Engine compartment
6: Under vehicle
7: Roof boxes
8: Trailers

Searchers:

Name of male officer: ....

Signature of male officer: ....

Name of female officer: ....

Signature of female officer:...

ANNEX J: LIST OF DANGEROUS GOODS

The following list refers to United Nations classifications.

Class 1, Division 1.1	Explosives
Class 1, Division 1.2	Explosives
Class 1, Division 1.3	Compatibility group C explosives
Class 1, Division 1.5	Explosives
Class 2.1	Flammable gases in bulk
Class 2.3	toxic gases (excluding aerosols)
Class 3	Flammable liquids in bulk of packing groups I and II
Class 3 and Class 4.1	Desensitised explosives
Class 4.2	goods of packing group I in bulk
Class 4.3	goods of packing group I in bulk
Class 5.1	Oxidising liquids in bulk of packing group I
Class 5.1	Perchlorates, ammonium nitrate and ammonium nitrate fertilisers, in bulk
Class 6.1	toxic substances of packing group I
Class 6.2	Infectious substances of Category A
Class 7	Radioactive material in quantities greater than 3000 A_1 (special form) or 3000 A_2, as applicable, in Type B or Type C packages
Class 8	Corrosive substances of packing group I in bulk

ANNEX K: DRILL/EXERCISE NOTIFICATION FORM

PORT AUTHORITY OF JAMAICA

FACILITY DRILL/EXERCISE NOTIFICATION *

This serves as official notification that the facility listed below will be conducting training (Drill/Exercise) as required under Part 'B' sections 18.5 and 18.6 of the ISPS Code.

1. General Facility Information

Name Of Facility	
Location Of Facility	
Port IMO Identification Number	
Contact Person (S)	

2. Training Information

Date Training Will Be Conducted	
Time Training Will Be Conducted	
Type Of Training (State Drill Or Exercise)	
Type Of Drill (e.g. Access Control, Ship Security etc.)	
Name Of Drill/Exercise Coordinator	
Contact Number For Drill/Exercise Coordinator	

Any changes to the above information will be communicated at least twenty-four (24) hours prior to the date indicated above for the commencement of the drill or exercise.

Name: ______________________

Position: _________________________

Date: _____________________________

* (i) This notification is to be submitted not less than seven (7) days prior to the scheduled drill/exercise date.

(ii) The Port Authority Of Jamaica reserves the right to attend and observe the above training.

ANNEX L: DRILL/EXERCISE REPORT FORM

PORT AUTHORITY OF JAMAICA
FACILITY POST DRILL/EXERCISE
ANALYSIS*

The facility listed below has conducted a training (Drill/Exercise) as required under Part ‘B’ sections 18.5 and 18.6 of the ISPS Code. The following is an analysis of the results.

1. General Facility Information

Name Of Facility	
Location Of Facility	
Port IMO Identification Number	
Contact Person (S)	

2. Training Information

Date Training Was Conducted	
Time Training Was Conducted	
Type Of Training (State Drill Or Exercise)	
Area Of Plan That Training Tested (e.g. Access Control, Ship Security etc.)	
Name Of Drill/Exercise Coordinator	
Contact Number For Drill/Exercise Coordinator.	
Brief Description Of The Drill/Exercise	

Brief Description of Weakness Noted.	
Brief Description of Corrective Actions Taken.	

Name: ______________________

Position: _________________________

Date: _____________________________

* (i) This form must be submitted within seven (7) after the drill/exercise.