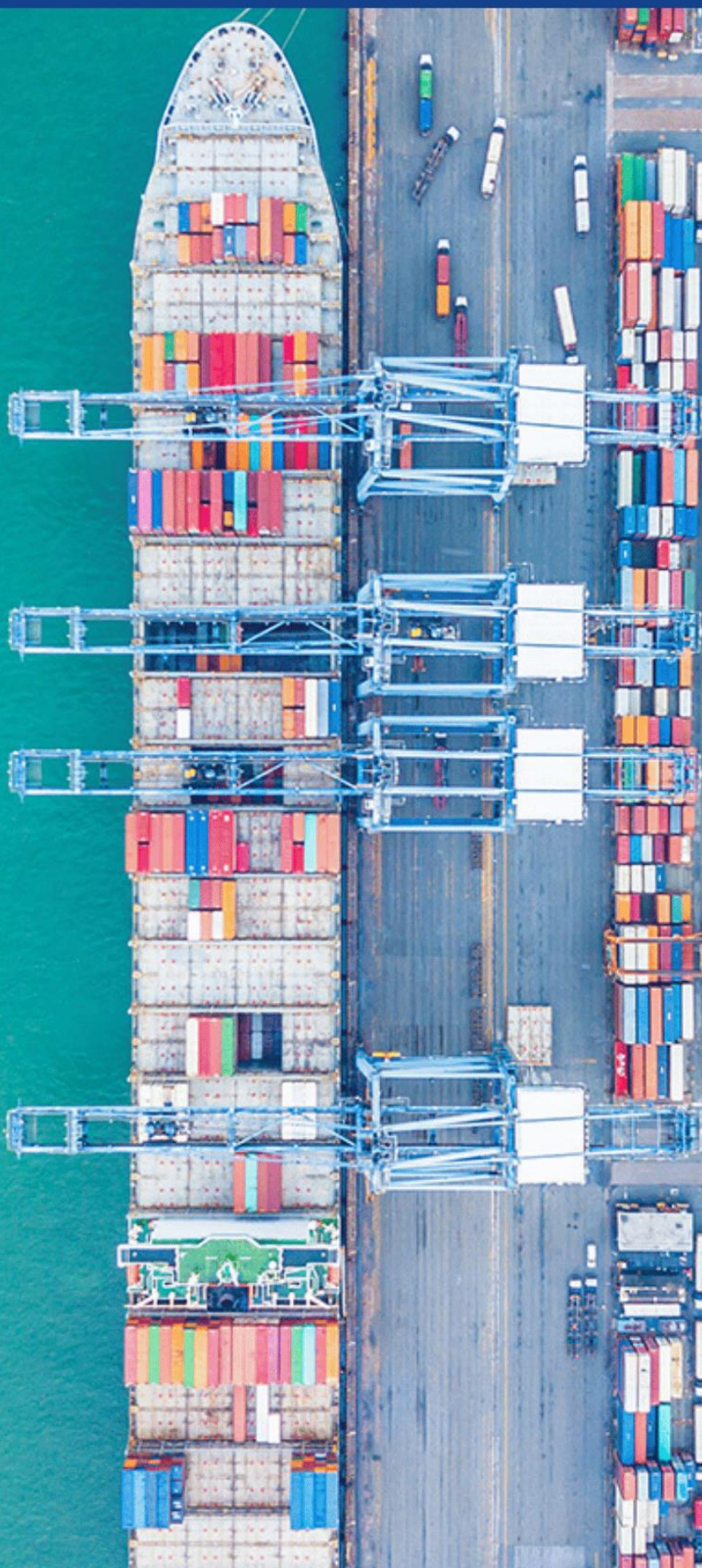
ASEAN REGIONAL FORUM

Promoting peace and security through dialogue and cooperation in the Asia Pacific

ASEAN Regional Forum Compendium of Best Practices on the Implementation of the International Ship and Port Facility Security Code



2025

About the Compendium

From 2022 to 2024 the Governments of India, Papua New Guinea, the Philippines, and the United States of America co-chaired a three-part "International Ship and Port Facility Security Code Training Series" under the auspices of the ASEAN Regional Forum (ARF). The objective of the ARF training series was to increase understanding and implementation of the requirements under the International Maritime Organization's (IMO) Safety of Life At Sea Convention on International and Ship and Port Facility Security (ISPS) Code.

The training series included lectures by Member State representatives and other subject matter experts, plenary and breakout group discussions among practitioners, as well as training drills and site visits to various port facilities.

- Part 1 was hosted at IMO headquarters in London, United Kingdom, on 5-9 September 2022 and addressed the ISPS Code topics of access control, perimeter control, and lighting.
- Part 2 was hosted in Mumbai, India on 10-14 April 2023 and addressed ISPS Code topics of guards and police, trainings and procedures, security infrastructure, and cyber risk management.
- Part 3 was hosted in Port Moresby, Papua New Guinea on 23-25 April 2024 and focused on ISPS Code topics of communications, robust national architecture for port security, implications of piracy on maritime security and ISPS code adherence, documents and forms, and electronic surveillance.

Throughout the engagements, ARF countries worked together to identify good practices from ports within the ARF, including practical drills and exercises, and identify key resources for effective port management and security. During Part 3, participants also worked together to develop and provide inputs into a virtual compendium of best practices from the series.

This compendium compiles many of the best practices identified over the course of the training series. Presentations and other materials from the three training sessions are available on their respective websites:

1. https://sites.google.com/meridian.org/arfportsecurity/home
2. https://sites.google.com/view/arfportpart2workshop/home
3. https://sites.google.com/view/arfportpart3workshop/home

This compendium was produced to ensure those practices are captured and disseminated for use by all ARF Members. The compendium is intended to further the goals under the 2022-2026 ARF Maritime Security Work Plan, Priority area 3: Capacity Building and Enhancing Cooperation of Maritime Law Enforcement Agencies in the Region and to serve as a concrete deliverable following the conclusion of the three-part training series as approved at the 26th ARF Ministerial Meeting in Thailand on August 2, 2018.

Part 1 participants outside IMO Headquarters in London, United Kingdom (upper left); Part 2 participants debrief a training drill at the Jawaharlal Nehru Port, Navi Mumbai, India (upper right); Part 2 participants debrief a training drill at Mumbai Port, Mumbai, India (lower left); Part 3 participants gather for a group photo in Port Moresby, Papua New Guinea (lower right)

CONTENTS

I. Communications

Best Practice: Community Alliance Program

Category:	Communications
Location:	Shell Tabangao Refinery Batangas, Luzon, Philippines
Date Observed:	19 July 2005
PoC:	Mansueto Flores Facility Security Manager

Description: The Community Alliance Program is a partnership with five local "barangays" or neighborhoods bordering the port facility. The company funds public works projects in these communities and has fostered a community watch program. This program has resulted in an increased level of vigilance and reporting of suspicious activity as well as a marked reduction in pilferage from the port facility.

Discussion: This program has resulted in an increased level of vigilance and reporting of suspicious activity as well as a marked reduction in pilferage from the port facility. Most of the facility workers are from the neighborhoods being helped.

Potential Down-side: Neighborhoods may become dependent on funds provided. Once started, the facility may feel obligated to increase funding of projects because of a threat of public backlash.

Conclusion: The Community Alliance Program is beneficial to all involved. Not only in supported neighborhoods whose borders touch the facility's fence line but also by creating a "protective bubble" around the facility.

Cost: Overall cost depends on the size of projects funded and the savings realized through the reduction in pilferage. Costs of the public works projects are shared by all members of the program which keeps costs down.

Best Practice: Residential Outreach Program

Category: Communications

Location: B12 Petroleum, Vietnam

Date Observed: August 2006

PoC: Nguyen Dang Oanh
Tel: 033 846446

Description: Residential outreach program that encourages neighboring facility residents to report suspicious activity.

Discussion: The landside fence line of the B12 Petroleum facility runs along the base of a steep hill which rises approximately 150 feet above sea level. Atop this hill is an extensive housing development whose residents have a commanding view of the facility. The facility's security management team developed an outreach program that provides local residents with a 24-hour emergency number, a point of contact, and monetary incentives to all who report observing any suspicious activity. The facility holds regular meetings with the residents to allow ideas or concerns to be expressed.

Potential Down-side: No potential downside identified.

Conclusion: The residential outreach program is an effective method of enlisting the participation of citizens to help with security.

Cost: Cost of implementing this practice is unknown.

II. Cybersecurity

Best Practice: Cyber Incident Recovery at the Container Terminal in Indonesia

Category:	Cybersecurity
Location:	Tanjung Priok Container Terminal Jakarta, Indonesia
Date Observed:	17 November 2022
Website:	www.priokport.co.id

Description: In 2022, cyber-attacks occurred at Tanjung Priok Container Terminal in Indonesia, causing the container terminal at the port to halt operations for 21 hours. The port gradually resumed operations and systems were restored successfully.

Discussion: Please be reminded to regularly review cyber incident recovery playbook as the guidance for cyber incident recovery and perform cyber incident recovery drills to prepare for cyber-attacks. High-profile cyber-attacks against the maritime industry and ports demonstrate the need to stay alert and be proactive to prevent cyber-attacks. Make sure all systems in your business environment are patched and up-to-date. Below are a few best practices recommended by the Center for Internet Security, to prevent and limit the impact of cyber-attack:

- Maintain backups using 3-2-1 backup best practices.
- Develop plans and policies to ensure IT security in accordance best practices.
- Regularly review firewall and security infrastructure perimeter settings.
- Harden your endpoints including servers and PC clients.
- Keep systems up to date.
- Train the cyber security incident response team.
- Review your cyber incident recovery playbook regularly
- Perform cyber drills regularly as required.
- Perform IT security and phishing awareness exercises regularly.

Potential Down-side: The system could be expensive to install and require IT personnel to be on-call or on duty 24/7 to respond to any cyber-attack.

Conclusion: A port facility has cyber resilience if it can defend itself against these attacks, limit the effects of a security incident, and guarantee the continuity of its operation during and after an attack.

Cost: The cost of installing the application would require an initial investment. The cost of routine maintenance will be fairly low.

Best Practice: Maritime Industry Cybersecurity Resource Center

Category:	Cybersecurity
Location:	United States of America
Date Observed:	2023
PoC:	MaritimeCRC@uscg.mil

Description: The website is a collaborative effort between the U.S. Coast Guard, U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), and U.S. Department of Transportation Maritime Administration (MARAD) to ensure current maritime cyber threat information is available to the public and stakeholders.

Discussion: The website is a single-source hub for Marine Transportation System related cybersecurity resources. The site provides current information related to reporting cyber incidents, relevant policies and guidance, cyber-related bulletins and alerts, and links to other useful sources.

Potential Down-side: Website requires routine maintenance to ensure information is current, accurate, and pertinent to maritime port partners.

Conclusion: The 2023 U.S. Coast Guard Area Maritime Security Annual Report identifies cybersecurity as one of the top focal points for the U.S. Coast Guard Area Maritime Security Committees. Collaborative information sharing, such as this resource center website, helps the maritime industry keep abreast of new information, policies, and points of contacts for enhancing cybersecurity. Additional information on the annual report can be found at: www.news.uscg.mil/maritime-commons/Article/3959105/area-maritime-security-committees-2023-annual-report/

Cost: Unknown

Best Practice: Have a Robust Cybersecurity Strategy

Category:	Cybersecurity
Location:	Jawaharlal Nehru Port Authority, DP World India
Date Observed:	2018
Website:	www.jnport.gov.in

Description: To have a robust cyber-security strategy.

Discussion: To have a layered approach in cyber-security strategy, where penetration at layer above activates defence mechanism in the layer below. The different layers of cyber security at JNPA–DP World are as follows:

- Perimeter security is a layered defence mechanism in cybersecurity that protects a network or system from external threats. It includes security protocols, access controls, and firewalls. Perimeter security aims to detect potential threats, deter intruders, and delay unauthorized attempts to breach the boundaries.
- Network security protects your network and data from breaches, intrusions, and other threats. It describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection. It includes antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), VPN encryption, etc.
- Endpoint security is a type of cybersecurity that protects devices that connect to an organization's systems and infrastructure, such as desktops, laptops, mobile devices, and tablets. Endpoints can be entry points to organizational networks that can be exploited. Endpoint security protects these entry points from malicious attacks.
- Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification. Authorization, authentication, and encryption are some of the application security features.
- User security is important because it helps organizations, and their users, protect employee, customer, and corporate data from threats, financial loss, and identity theft. Strong end-user security hygiene can also support regulation compliance, prevent reputational damage, and preserve customer trust.
- Data security is the process of protecting digital information from corruption, theft, or unauthorized access throughout its entire life cycle. It covers hardware, software, storage devices, user devices,

access and administrative controls, and organizations' policies and procedures.

- Governance layer provides a strategic view of how an organization controls its security, including defining its risk appetite, building accountability frameworks, and establishing who is responsible for making decisions. Effective governance will also ensure that cyber security activities help to support the organization's strategic goals.

Potential Down-side: While cyber security strategies may have similar elements and approaches, what works for one area may not be appropriate or adequate for another. Hence, organizations should conduct a detailed assessment to ensure the most appropriate and effective cyber security strategy is chosen and incorporated.

Conclusion: Port facilities globally are becoming increasingly complex and dependent on the extensive use of information and communications technologies. For example, the use of autonomous equipment, berthing operations, etc. Some of this technology is embedded in the fixed and mobile assets of the port, while some are remotely located, such as the systems used to administer vessel movements and traffic. Hence, it is essential that cyber security strategies be considered an integral part of a holistic approach throughout an asset's lifecycle management. Financial, reputational, and safety consequences may arise if cyber threats are not adequately addressed. Such impacts should also be considered.

Cost: Costs are variable depending on various factors, including the region where the solution is being implemented, resilience of the system being developed, backup arrangements being sought, etc.

Best Practice: Have a Robust Cybersecurity Risk Management Framework

Category:	Cybersecurity
Location:	Jawaharlal Nehru Port Authority, DP World India
Date Observed:	2018
Website:	www.jnport.gov.in

Description: To have a robust cyber-security risk management framework.

Discussion: Container terminal operator DP World in Jawaharlal Nehru Port Authority uses the U.S. Department of Commerce's National Institute of Standards and Technology's (NIST) Cybersecurity Framework. The NIST Cybersecurity Framework helps organizations better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help decide where to focus your time and money for cybersecurity protection. One can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover, which are described as follows:

- Identify: List all equipment (laptop, tablets, smart phones, POS, etc), software, data used, etc. Ensure cybersecurity policy covers all aspects and take steps to protect from attacks and limit damage if one occurs.
- Protect: Includes access control, using security software, encrypting data, conducting regular back-ups, policy for data handling, training of employees.
- Detect: Includes continuous monitoring of devices from unauthorized access, or software. Investigating any unusual activity in the network, including unauthorized connections.
- Respond: Includes notifying those whose data may be at risk, investigating the attack, reporting the attack to authorities, incorporating lessons learnt in the cyber-security plan.
- Recover: Involves recovering after an attack. It includes repairing and restoring the equipment and parts of network which were affected by the attack, as well as keeping employees and customers informed of the response and recovery activities.

Potential Down-side: The port may have existing cyber-security risk management frameworks, which would need to either be strengthened or develop a framework in line with global standards, allowing scaling with time.

Conclusion: Nowadays, ports are continually increasing their exposure through

autonomous operations, and it is imperative that they adopt appropriate cybersecurity risk management frameworks as part of their overall cybersecurity strategy.

Cost: Costs are variable depending on various factors, including the region where the solution is being implemented, resilience of the system being developed, backup arrangements being sought, etc.

III. Documents and Forms

Best Practice: ISPS Code Handbook

Category:	Documents and Forms
Location:	Chittagong Port Authority Bangladesh
Date Observed:	15 October 2005
PoC:	Cpt K. M. Jashimuddin Sarker Facility Security Manager Phone: 031 9553584

Description: The Designated Authority Committee published a handbook describing the duties and responsibilities of Port Facility Security Officers and Security personnel at differing levels of security within the port.

Discussion: The handbook was given to each port employee. It ensures all employees are aware of the differing levels of security and the procedures called for when security levels are raised. This awareness has led to increased cooperation of all port employees during mandatory drills and exercises.

Potential Down-side: In the wrong hands, the handbook could be used by persons wishing to circumvent security measures to gain access to the port.

Conclusion: Port employees are familiar with the steps taken when raising the security level of the port. In addition, all personnel are aware of their duties and responsibilities associated with changing security levels and the importance of the International Ship and Port Facility Security Code.

Cost: The cost of publishing the handbooks is minimum.

Best Practice: Security Level Increase Checklist

Category:	Documents and Forms
Location:	Chittagong Port Authority Bangladesh
Date Observed:	15 October 2005
PoC:	Cpt. M. Quamrul Hossain Chittagong Port Authority Phone: 88 011 246153 E-mail: mocpa@cpa.gov.bd

Description: Checklists with step-by-step instructions for increasing the security levels are posted at entry gates to the port. They contain detailed procedures for raising the security level from one level to the next and are printed in Bangla. The checklists are taken from the approved Port Facility Security Manual.

Discussion: The Chittagong Port Authority printed checklists and posted them in each guard post at the entries to the port. The checklists are printed in Bangla to ensure guards fully understand the steps to take to increase security levels according to the Port Facility Security Plan. Gate guards are fully aware of their duties when increasing the security level and the additional security checks to be performed.

Potential Down-side: Information contained on the checklists could be used to circumvent security if they fall into the wrong hands.

Conclusion: Checklists are an effective means to ensure security personnel from different agencies understand the measures to take when increasing a port's security level.

Cost: Moderate cost to cover printing

IV. Electronic Surveillance

Best Practice: Portable Explosive Vapor Detector

Category: Electronic Surveillance
Location: Kandla, India
Date Observed: May 2005

Description: Portable explosive vapor detector

Discussion: The port purchased a portable explosive vapor detector to assist guards in assessing the atmosphere in vehicles, containers, boxes, packages, and on the clothes of people. The hand-held digital device tests for the presence of a variety of volatile chemicals associated with the manufacture of various explosives including TNT, NG, PETN, RDX, and EGDN. The port has not had an incident in which the explosive vapor detector revealed any suspicious material. Detectors of various brands can be programmed to alert either silently or with an audible tone. Sealed shipping containers can be tested by using an elevated platform to place the sensor of the explosive vapor detector at a container vent near the top of the container. Detectors can be used to assess every vehicle and container entering a port, or only on suspicious vehicles and containers as part of a response protocol.

Potential Down-side: Cost and maintenance of commercial units is relatively high. Reliance in any high-tech tool can sometimes cause personnel to neglect basic search techniques. Each make and model of explosive vapor detector will detect different types of explosives. Detectors may not detect vapors of improvised explosives, including pipe bombs, flammable gas cylinders, or gasoline and home-made napalm.

Conclusion: An explosive vapor detector is a very valuable tool to have in a security tool-box, so long as security personnel recognize its technical limitations and do not neglect other search and detection techniques.

Cost: Varies between USD 1,500 and USD 3,000.

Best Practice: Electronic Tracking System

Category:	Electronic Surveillance
Location:	Hong Kong International Terminal & Modern Terminals, Ltd.
Date Observed:	October 2004

Description: Electronic tracking system for vehicles.

Discussion: Both terminals utilize an electronic tracking system linked to each vehicle used for transporting containers. This includes trailers and container pickers. At any given time, the terminal's command centers are capable of determining the exact position of one of these vehicles and establishing its current operations and/or future orders. Verification of the vehicle's current location can be conducted by use of closed circuit television cameras capable of identifying any vehicle anywhere on either terminal.

Potential Down-side: Implementing this type of tracking system is costly and requires computer maintenance and training of personnel.

Conclusion: This type of technology may not be necessary at smaller facilities, but it significantly increases monitoring capabilities and efficiency at larger terminals. Initial and on-going costs could be prohibitive for smaller operations.

Cost: Initial installation, training and maintenance costs can be significant. A cost/benefit analysis would be necessary for smaller terminals before implementing this type of technology.

Best Practice: Video Surveillance System (CCTV)

Category:	Electronic Surveillance
Location:	Manila International Container Terminal, Port of Manila, Philippines
PoC:	Menandro D. Cariaga Head, Security and Surveillance Department Email: mcariaga@ictsi.com

Description: Video surveillance system (CCTV).

Discussion: Video surveillance systems are crucial in port security and in compliance with the International Ship and Port Facility Security (ISPS) Code for several reasons:

- Deterrence: CCTV cameras deter criminal activity by providing a visible reminder that the area is being monitored.
- Detection: Cameras can detect suspicious activities, unauthorized access, or breaches in security protocols in real-time.
- Investigation: In case of security breaches or incidents, CCTV footage provides valuable evidence for investigation, identifying perpetrators, and understanding the sequence of events.
- Situation Awareness: CCTV allows security personnel to monitor activities across different areas of the port facility in real-time, enabling quick response to any security threats or emergencies.
- Compliance: The ISPS Code mandates the implementation of security measures to enhance the safety and security of ships and port facilities. CCTV surveillance is often a requirement for compliance with these regulations.

Overall, CCTV surveillance systems play a vital role in enhancing security, preventing incidents, and ensuring compliance with international security standards in ports. The cameras are Internet Protocol based with analytics to detect violations and trigger alarms.

Potential Down-side: While CCTV surveillance systems offer numerous benefits for security and monitoring, there are also potential downsides to consider:

- High Cost – The systems require expensive equipment, installation and maintenance.

- Technical issues – They are prone to issues such as malfunctions, systems failures, and compatibility failures.
- False alarms – CCTV systems can be triggered by false alarms such as animals or environmental factors, which can lead to unnecessary disruptions and wasted resources. This can also lead to complacency among security personnel making them less responsive to genuine security threats.
- Privacy concerns – Access control involves the use of cameras and other surveillance equipment, which can raise privacy concerns among individual and/or violation of the Data Privacy Act.
- Maintenance – These systems require regular maintenance and upkeep to ensure they are functioning properly. This can be time-consuming and expensive, especially for larger systems with different access points and cameras.
- Human error – This can include mistakes in programming, forgetting to lock doors or not monitoring the system closely enough.

Conclusion:

Automated access control and video surveillance systems are both significant components of a comprehensive security system as they allow for more efficient and effective response to potential threats. Automated access control systems enable personnel, visitors, and other stakeholders to easily gain access into the premises but make unauthorized entry more difficult. Breaches can be easily detected and entry to certain areas controlled, minimizing the risk of unauthorized access and potential security breaches.

CCTV systems provide valuable visual evidence in case of security incidents, aiding in investigation and improving overall security. While it may have drawbacks such as high cost of installation and maintenance, privacy concerns, and human error, the benefits of having said system outweighs these disadvantages.

Cost:

The initial cost of a surveillance system is PHP 90M. This amount covers the end-to-end solution for the supply, delivery, and installation of the major components of the system like the latest Internet Protocol cameras and intelligent video management system with analytics.

Best Practice: Video Surveillance System with Video Analytics

Category:	Electronic Surveillance
Location:	Singapore
Date Observed:	August 2021
PoC:	Muhammad Aminoor, Maritime and Port Authority of Singapore

Description: The video surveillance system at the port facility is fitted with video analytics to enhance the surveillance of the premise. The system triggers a pop-up alert on the monitor screen to notify the security officer of a detection within an area of concern and for the security officer to conduct checks either by panning the camera or deploying ground assets to investigate.

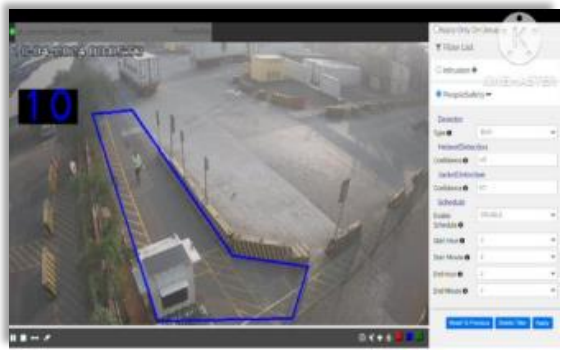
Discussion: With technology advancements, such video analytic capabilities have helped security officers increase their productivity, by handling multiple tasks at one time, reducing burden and fatigue by the end of the security officer's shift.

Potential Down-side: The video surveillance system could be costly depending on how complex the detection capability is and the extent of coverage for the port facility. The system requires a high level of maintenance and would need to be upgraded to keep up with new technology advancements.

Conclusion: A sizeable number of port facilities in Singapore have added video analytics capabilities to their video surveillance system. It helps reduce fatigue for the security officers as they do not need to monitor the screens all the time and only need to focus on alerts triggered by the system.

Cost: Not available.

Best Practice: To Incorporate Video Analytics System



Category:	Electronic Surveillance
Location:	Jawaharlal Nehru Port Authority, DP World India
Date Observed:	2022
Website:	www.jnport.gov.in

Description: To incorporate video analytics system.

Discussion: Container terminal operator DP World in Jawaharlal Nehru Port Authority uses a video analytics system to ensure compliance with various terminal safety regulations. Video analytics is a technology that processes a digital video signal using a special algorithm to perform a security-related function. There are three common types of video analytics: fixed algorithm (an algorithm is a set of instructions that a computer follows to solve a problem) analytics, artificial intelligence learning algorithms, and facial recognition systems.

The first two of these try to achieve the same result. That is, they try to determine if unwanted or suspicious behavior is occurring in the video camera's field of view and the algorithm notifies the console operator of the finding. However, each takes a dramatically different route to get to its result. Fixed algorithm analytics use an algorithm that is designed to perform a specific task and look for a specific behavior. For example, common behaviors that fixed algorithm analytics look for include: crossing a line, moving in the wrong direction, speeding, etc. Artificial intelligence learning algorithms operate entirely differently. Learning algorithm systems begin as a blank slate. They arrive completely dumb. After connecting to a given camera for several weeks, they begin to issue alerts and alarms. During that time period the system is learning what is normal for that camera's image during the day, night, weekday, weekend, and hour by hour. After several weeks, the system begins to issue alerts and alarms on behavior in the screen that it has not seen before or that is not consistent with what it has seen during that time period for that day of week.

The third type of analytic is facial recognition. Facial recognition systems can be used for access control or to help identify friend or foe. Facial recognition systems can also be used to further an investigation. Typical facial recognition systems match points on a face with a sample stored in a database. If the face does not match a record, it will try to create a new record from the best image

available of that person. These are capable of making real-time matches of one image against many.

Video analytics systems in the port have CCTV cameras covering the entire yard, which are linked with AI logic software to detect any non-compliance of the safety regulations. When non-compliance is detected, it delivers an alert over a public address system positioned at each camera instructing the offending person of their actions and to immediately rectify these. This alert may be issued in different languages and is recorded in the data log for evaluation. All incidents are monitored from a central control room and conveyed to the areas' supervisor to ensure total compliance and for necessary action to avoid recurrence.

Potential Down-side: Video analytics systems are not standalone systems. The organization needs to develop an entire ecosystem for video analytics to effectively operate and give intended results. For example, the organization may need to train employees to be responsive to alerts.

Conclusion: Video analytics systems are a must-have to ensure continuous round-the-clock monitoring of port areas and compliance with applicable rules and regulations, which otherwise may not be possible. Such systems can also contribute to developing a safety culture in port operations that extend beyond the monitored areas.

Cost: Costs are variable and depend on a number of factors, such as the region where the solution is being implemented, and availability of the OEM in the area, size of the area, factors incorporated in the ecosystem.

Best Practice: To Incorporate Gate Automation System

Category:	Electronic Surveillance
Location:	Jawaharlal Nehru Port Authority, DP World India
Date Observed:	2022
Website:	www.jnport.gov.in

Description: To incorporate gate automation system.

Discussion: Automated smart gates can help ensure effective and efficient flow of imports and exports through the terminal's gates, minimize human-machine interface, and ensure all required information is captured by the terminal.

These gates consist of a pre-gate optical character recognizing (OCR) enclave housing cameras that capture images of the inbound and outbound container's distinct alphanumeric code. The system converts that information into digital information, which is then passed on to the terminal's database and transmitted to the terminal gates.

This ensures that the truck/container's information is digitally available prior to reaching the gate. The gate system can recognize and verify the container and upon validation, permit it to enter or depart the terminal automatically without human intervention. The system can also allocate trucks with drop-off or pick-up locations as needed.

Such systems expedite and improve the efficiency of port operations as well as the digital record keeping of the cargo movement to/from port.

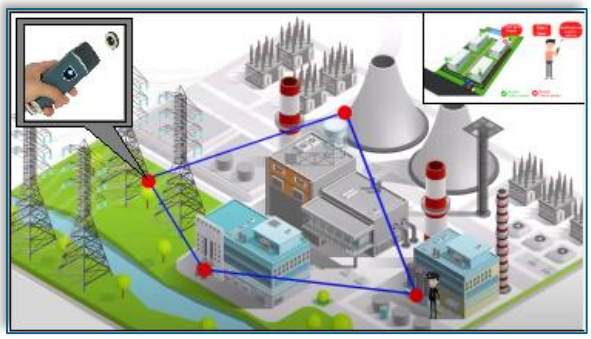
Potential Down-side: The organization may have to check local regulations as some countries do not allow automatic gate operation in ports. However, even in such countries this system would ensure that the person on duty at the gate would get all the information prior to arrival of the container and/or truck and expedite the entire operation.

Conclusion: Automatic gate operation enhances port efficiency, and if coupled with vehicle monitoring systems and radiation detectors, can provide a complete solution for passage of containers and/or trucks to/from ports.

Cost: Costs are variable and depend on a number of factors, including the

region where the solution is being implemented, availability of the equipment in the area, size of the area, and factors incorporated in the ecosystem.

Best Practice: Security Checkpoint Systems



Category: Electronic Surveillance
Location: Unnamed U.S. Facility
Date Observed: 2023

Description: Checkpoint system to verify roving security surveillance.

Discussion: Security guards and personnel with security duties can utilize a checkpoint system consisting of touch checkpoints marked with RFID tags or QR codes along patrol routes to ensure oversight of specific locations at designated times. When the checkpoint is touched with an issued device, the system records the time and location, ensuring all checkpoints are visited, providing a record of patrol.

Potential Down-side: Requires resource investment into the technology for the checkpoint system and secure cyber networks to protect the information from unauthorized access.

Conclusion: The rotation of the checkpoints can be randomly changed as part of a Random Antiterrorism Measure (RAM) program. RAM changes the security atmosphere of a facility. When implemented in a truly random fashion, RAMs alter the external appearance or security signature of a facility in order to disrupt potential attackers (or criminals) conducting surveillance operations in order identify security patterns and potentially evade detection during the execution phase of a planned operation.

Cost: Unknown.

V. Guards and Police

Best Practice: 24 Hour, Seven Days A Week Security Manning

Category:	Guards and Police
Location:	Muara Port, Brunei Darussalam
Date Observed:	19 March 2024
PoC:	Port Facility Security Officer

Description: Access to the facility is manned 24/7 by security guards, police and port operator security teams, and continuously monitored by CCTV cameras.

Discussion: Security guards supplemented with additional security personnel conduct roving security and foot patrols at hourly intervals during the day and night. The facility varies the security patrol times and routes to avoid establishing routines.

Potential Down-side: Can be costly due to additional security personnel deployment for a small facility.

Conclusion: Considering the facility's size and operational volume, the current security measures are sufficient to maintain the security, safety and operations of the facility.

Cost: Not available.

Best Practice: Police Officer Stationed on Facility 24 Hours Per Day

Category: Guards and Police

Location: Laem Chabang, Thailand

Date Observed: July 2005

Description: The port of Laem Chabang entered an agreement with the local municipality to provide a police officer and police motorcycle at the facility 24 hours a day, seven days a week.

Discussion: Guard forces are limited in many ways. In most countries, security guards do not have arrest authority. If guards engage a violator, they can attempt to detain them until the police arrive. In many instances guards do not have the training nor equipment necessary to detain a violator. Local police officers may be too distant, or otherwise busy, and unable to quickly respond to calls for assistance. Guards typically do not have vehicles with emergency equipment (lights and siren) that they can use to stop or pursue a fleeing vehicle. Guard forces typically do not have access to computerized databases to check the criminal or driver's license status of a suspicious person or violator, or to check the status of a license plate. The presence of a guard force typically does not present the same deterrent effect against crime as does the presence of police officers. This facility overcame these issues by entering into an agreement with the local police to have a police officer stationed at the facility 24 hours a day, seven days a week. The facility had the police officer park his motorcycle at the main entrance as a visible deterrent to crime.

Potential Down-side: Cost and availability. Most municipalities will not assign a police officer to a private facility unless the facility covers the cost of the officer's pay, benefits, and vehicle. In some cases, even if a facility is willing to pay the costs of having an officer assigned at the facility, police personnel shortages or policy may prevent the municipality from assigning a police officer to a facility.

Conclusion: For facilities that are distant from a police station or that have a large amount of crime, hiring a police officer to work at the facility can be a very effective approach to improving security. Costs savings can be achieved by hiring a police officer at the facility for only limited hours each day.

Cost: Expensive, depending on the hours an officer is hired to work.

Best Practice: 24 Hour, Seven Day A Week Dispatch Center

Category: Guards and Police

Location: Port of Bangkok, Thailand

Date Observed: June 2005

Description: The facility maintains a 24/7 dispatch center with at least two staff on duty at all times.

Discussion: The facility takes a proactive approach to having a centralized facility security and safety dispatch center. At least two dispatch personnel are assigned at all times. There is a bunk room attached so that during quiet times, one dispatcher can rest while the other maintains the radio watch. The dispatch center includes telephones, faxes, and VHF radios, with radio frequencies shared with police, fire, and the Navy. A large display board lists phone numbers for key agencies and personnel, including the work, cell, and home numbers of facility officials. Phones on the facility can reach the dispatch center by calling a four-digit number, to expedite connection. Dispatchers maintain a detailed radio logbook documenting all incidents routed through them. The facility has full back-up power in the event of a municipal power outage. In many facilities, dispatchers also monitor facility CCTV cameras and alarms. Collateral benefits for a 24/7 dispatch center include enhanced emergency fire, safety, and medical response.

Potential Down-side: Can be expensive for a small facility.

Conclusion: For moderate or large facilities, a dispatch center is a valuable way to coordinate security forces and to provide an effective public/security/law enforcement interface. Providing 24/7 dispatch support can significantly enhance security, safety, and operational efficiency.

Cost: Unknown.

Best Practice: Deployment of Female Philippines Coast Guard Radio Operators

Category:	Guards and Police
Location:	Philippines
PoC:	Philippine Coast Guard Coast Guard Districts
Website:	https://coastguard.gov.ph

Description: Female Philippine Coast Guard (PCG) Radio Operators

Discussion: The PCG came up with a policy on the deployment of female PCG personnel as radio operators, particularly in high-risk areas. These female PCG radio operators are dubbed the “Angels of the Sea”. The Angels of the Sea were first deployed in Coast Guard District Southwestern Mindanao, which covers the area along the Basilan Strait and Sibutu Passage, to temper seafarers' anxieties at the height of piracy and kidnapping in the areas. The aim of the program is to “ease the tension” when communicating with foreign vessels. Likewise, the Angels of the Sea were also conceptualized to provide equal opportunities to all members of the uniformed service so they could play their niche roles in securing the nation together as one at sea.

Conclusion: This initiative on the part of PCG has proven effective in helping to ease the tension experienced by victims during critical maritime situations allowing them to communicate more comfortably and audibly with PCG.

Cost: Cost associated with training, equipment, and logistical requirements for the operation.

Best Practice: Deployment of Sea Marshals Onboard Domestic Passenger Vessels

Category:	Guards and Police
Location:	Philippines
PoC:	Philippine Coast Guard Maritime Security Law Enforcement Command
Website:	https://coastguard.gov.ph

Description: The Sea Marshal program is a deterrent mechanism for maritime terrorism, piracy, and armed robbery against ships at sea.

Discussion: The increase in the threat of maritime terrorism and piracy has compelled the Department of Transportation to issue a Department Order to expand the scope of operation of the Philippine Coast Guard's (PCG) Sea Marshal Group to all Coast Guard Districts and increase its function in the enforcement of laws as the lead agency for the National Task Force Sea Marshal. This Department Order mandates the PCG to organize, train, equip and maintain a specialized unit deployed both covertly and overtly onboard domestic passenger vessels. Its main objective is to protect voyages of passenger-laden vessels on domestic routes.

Potential Down-side: The presence of armed personnel onboard can create a negative implication on the level of security. While it is created to deter illicit activities, it may also be an opportunity for the criminals to take advantage of the presence of weapons in the hands of the enforcer.

Conclusion: This initiative on the part of PCG has proven effective not only in deterring maritime terrorism and piracy but also other illicit maritime activities such as smuggling and human trafficking. It provides an opportunity for the PCG to conduct rescue operations for individuals who are victims of human trafficking. It also allows PCG personnel to apprehend criminals while the vessel is underway.

Cost: Costs associated with specialized training on close quarters battle and hand-to-hand combat, equipment (weapons, gear, and other law enforcement paraphernalia), and other logistical requirements for operations.

Best Practice: Utilization of Community Intelligence Network

Category:	Guards and Police
Location:	Philippines
PoC:	Philippine Coast Guard
Website:	https://coastguard.gov.ph

Description: The Community Intelligence Network was conceptualized as a mechanism to expand the range and coverage of the Philippine Coast Guard's (PCG) human intelligence network in coastal communities.

Discussion: Among the initiatives of the PCG in building good rapport in their area of responsibility are community engagement operations. The PCG offers a free training to locals on "water search and rescue," basic life support, and a first responders' seminar. This activity allows the PCG to not only build a company of first responders but could also easily develop a well-established relationship with the community which creates an atmosphere of obligation on the part of those trained to be more cooperative in sharing relevant information. They now serve as the PCG's "eyes and ears" as well as force multipliers in intelligence gathering. The intelligence reports help the PCG design its courses of action in preventing the commission of crimes.

Potential Down-side: The initiative needs multiple sources to ensure accuracy of intelligence that is gathered. There will always be a degree of mistrust and disloyalty especially if it is a close-knit community.

Conclusion: This initiative on the part of PCG has proven effective in improving maritime security in coastal areas. People tend to hesitate to commit illicit activities for fear of being reported by law-abiding citizens. This can also develop a feeling of shame to break the good relationship by violating the law.

Cost: Cost associated with training, equipment, operationalization, and incentives.

Best Practice: Waterside Security

Category:	Guards and Police
Location:	Port of Manila, Philippines
Date Observed:	2024
PoC:	Philippine Coast Guard
Website:	https://coastguard.gov.ph

Description: Waterside security patrols along the anchorage areas.

Discussion: In recent years, enhanced security measures have made port infrastructure a hard target, deterring illicit groups. However, the focus of such groups has shifted to the anchorage area. Proactive waterside patrols by the Philippine Coast Guard (PCG) have helped to fortify these areas against security threats. Beyond traditional patrols, the strategic deployment of small boats has been a pivotal enhancement to operational agility. These vessels enable rapid responses to security threats within the anchorage area. When supported by larger 'Mother Ships,' reach and endurance are extended, bolstering overall effectiveness. The approach has undergone rigorous testing, proving its efficacy. The persistent presence of patrol teams acts as a potent deterrent, dissuading attempts at illicit activities within the vicinity. However, should such attempts persist, swift response capabilities ensures prompt resolution, thereby upholding the security and integrity of the port.

Potential Down-side: Additional logistical expenses for both the port and the implementing agency.

Conclusion: Enhanced security measures in port anchorage areas have made them less appealing to illicit groups, but they remain focal points for security threats. Proactive patrols by the PCG deter such activities, supported by the strategic deployment of small boats and larger vessels. Despite additional logistical expenses for both the port and the implementing agency, these measures effectively uphold port security.

Cost: Costs relate primarily to fuel consumption for the PCG boats, which varies depending on the distance to the anchorage areas. Since the PCG already possesses boats, the overall expenditure remains relatively low.

Best Practice: High Power Spotting Scope

Category: Guards and Police
Location: Laem Chabang, Thailand
Date Observed: June 2005

Description: The Port of Laem Chabang employed an 80x magnification spotting scope on a tripod in an elevated office to improve their view of the entire port and approach channel.

Discussion: A high-power spotting scope in an elevated position offers several benefits over handheld binoculars. Spotting scopes of 60-100x magnification are 6 -10 times more powerful than binoculars. Their large diopter lens permits more light to enter the scope, enhancing low-light viewing. Using a tripod stabilizes the scope and greatly reduces small movements that can blur the vision in handheld binoculars. A spotting scope is far more effective at detecting persons, vehicles, or vessels at long distances and at seeing detail (e.g. license plate numbers, boat numbers, suspect physical features, etc.).

Potential Down-side: Spotting scopes need to be used on a tripod and are difficult to carry in the field. Monocular vision reduces the ability to discern the distance of an object.

Conclusion: For any facility that maintains an elevated position with a good view of their yards, docks, jetties, and waterways, the addition of a spotting scope can greatly enhance the ability of security officers and managers to detect security and safety threats to the facility.

Cost: USD 100 - 800, depending on quality and magnification.

VI. Lighting

Best Practice: Light Towers Double as Guard Towers

Category: Lighting
Location: Port of Cochin, India
Date Observed: May 2005

Description: Each of the more than 20 high power lighting towers on the facility are built with elevated platforms that permit guards or port officials to climb the towers and observe the port, adjacent waterway, and surrounding area from an elevated position.

Discussion: Building light towers that double as elevated observation platforms offer a port facility a number of advantages, including significantly enhanced security. In the event of a security breach, guards or law enforcement can use the towers to detect intruders on the facility. In the event of an attack on a facility, the elevated towers offer guards or law enforcement an elevated tactical advantage against armed adversaries. Platforms on the light towers displayed above permit an excellent view both within the facility, and over the wall to the outside of the facility. Towers can also be used by port managers to assess operational efficiency of various port operations and aid the supervision of employees and contractors.

Potential Down-side: If not secured against unauthorized access, intruders or attackers can climb the towers and use the elevated position to shoot at employees or guards, and/or to observe security personnel approaching their positions. Access ladders must be closed and locked so that only authorized personnel can use them.

Conclusion: This is a very useful construction concept that doubles the function of the light towers and significantly enhances intruder detection and incident response.

Cost: Depending on height and type of construction, integrating an elevated platform on light towers can cost between USD 1,000-5,000 per tower.

Best Practice: Solar Powered Emergency Street Lights

Category: Lighting

Location: Port of Chennai & Eenore, India

Date Observed: May 2005

Description: Inside each gate, the port installed solar powered emergency streetlights to supplement port security lighting in the event of a power outage of the primary and secondary power sources.

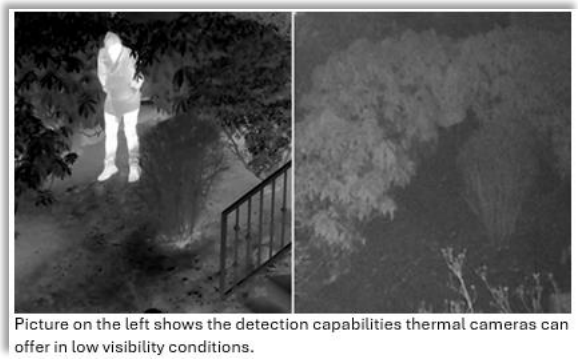
Discussion: Solar powered emergency streetlights consist of a photo-voltaic panel to collect solar energy and convert it into DC electricity, a bank of batteries to store the electricity, and a DC power light fixture to convert the stored electricity into lighting when other lighting is unavailable. The Ports of Chennai and Eenore used these lights at each of their facility entrances as backup to both their municipal electric and their diesel emergency electric generators. The solar lights require almost no maintenance, are long-lasting, and require no outside fuel source (except sunlight). Depending on the make and model, a fully charged light can provide light during 8-16 hours of darkness. Lights can be adjusted to automatically light at dusk, when municipal electricity goes out, or turned on manually.

Potential Down-side: Over time, batteries and photo-voltaic cells start to wear out. Deep cycle batteries have a life expectancy of 2- 5 years and are inexpensive to replace. Photo-voltaic cells have a life expectancy of 10-15 years, with a gradual loss of efficiency after five years. Extended weeks of cloudy or overcast weather can result in inadequate charging of the batteries.

Conclusion: In locations that receive an above average amount of sun, solar powered lighting can be an excellent emergency lighting source. The initial cost for purchasing the lights can be two to three times higher than lights attached to municipal electricity, but they reduce the need to run overhead or buried wires or install emergency electric generators as a back-up lighting source.

Cost: Approximately USD 2,000 per light fixture, including installation.

Best Practice: Thermal vs. Non-Thermal Camera Example



Picture on the left shows the detection capabilities thermal cameras can offer in low visibility conditions.

Category: Lighting
Location: Unnamed U.S. Facility
Date Observed: 2023

Description: Thermal camera for detecting personnel during low-light/night time conditions.

Discussion: Security lighting may provide both a real and psychological deterrent for continuous or periodic observation by an aggressor. Lighting is relatively inexpensive to maintain and may decrease the need for security personnel by reducing opportunities for surreptitious approach by potential attackers. Lighting must be compatible with video surveillance systems, as the cameras may need high intensity, low intensity, or infrared light for proper operation.

Potential Down-side: Requires resource investment into the technology for thermal cameras, video surveillance system and analytical software and secure cyber networks to protect the information from unauthorized access. Electronic surveillance systems require continual maintenance and upkeep to complement security staff.

Conclusion: Recapitalizing equipment aids enhancing overall lighting security measures.

Cost: Unknown.

VII. Perimeter Control

Best Practice: Light Pole Anti-Climb Guards

Category: Perimeter Control
Location: Port of Mumbai, India
Date Observed: June 2005

Description: Steel guards were welded to light poles outside the port's perimeter wall to prevent intruders from scaling the light poles to climb over the wall and into the port.

Discussion: The Port of Mumbai's security assessment indicated that municipal light poles directly outside the port perimeter walls were susceptible to being scaled, allowing an intruder to climb over the wall and into the port. The port designed curved and sharpened steel bars that were welded to a collar around the light pole. The curved steel bars are both a visual deterrent and effectively prevent a person from scaling the pole to a height where they could climb over the perimeter wall.

Potential Down-side: None. If the bars are not sufficiently strong or welded improperly to the pole, it is possible an intruder could scale the pole and break off individual bars using their body weight and arm strength.

Conclusion: This approach to securing intruder access from a telephone pole appears to be both effective and inexpensive to implement.

Cost: Materials – USD 20. Installation – USD 25-100 per pole depending on labor costs.

Best Practice: Continuing Fence Line into Water

Category: Perimeter Control

Location: Port of Kandla, India

Date Observed: June 2005

Description: The fence line is continued down the bank of the channel into the water to prevent trespassers from circumventing the fence to access the facility.

Discussion: At a waterfront facility, a common challenge to the effectiveness of walls and fences is the land/water interface and how to prevent intruders from walking around walls and fences at the waterline. This is especially problematic with tidal water, which floods and recedes, often leaving a gap at the end of the fence during low tide. At the Kandla Facility, this issue was addressed by continuing the construction of the security fence from the land down into the channel. At high and low tide, the fence creates an effective barrier against intruders. Lateral supports protect the fence against tidal movement or current.

Potential Down-side: A fence of this type is susceptible to flood damage and/or collecting trash from flooding and receding tides. The fence can still be circumvented by an intruder willing to go farther into the water to go over or around the fence. Constructing a fence in a waterway can be an expensive and time-consuming endeavor, especially if concrete footings are required.

Conclusion: For certain applications, especially those involving relatively still water, this can be an effective approach. This type of fence would not long survive fast moving (river or fast current) water. Depending on the type of construction and engineering required, this fence can be very expensive.

Cost: Varies considerably depending on size, geography and geology of the waterfront and the velocity of water flow.

Best Practice: Concrete Anti-Vehicle Barricades

Category: Perimeter Control
Location: Sriracha Harbor, Thailand
Date Observed: June 2005

Description: The Sriracha Harbor facility staged concrete barricades - sometimes called "Jersey Barriers" - adjacent to the entrance to their facility to be used to close the facility entrance in event of an elevated threat level.

Discussion: Concrete barricades are highly effective at stopping vehicles. This facility maintained five concrete barricades directly adjacent to their single entrance. In the event of an elevated threat level, the facility's security plan called for placing the barricades in front of the entrance, closing it to vehicle traffic. The barricades are relatively inexpensive to purchase or manufacture. They are moved by large fork-lift truck or other heavy equipment with appropriate harness. Concrete barricades should be constructed with easy-use lifting points so they can be quickly positioned. As above, barricades can be painted in bright colors to make them highly visible or with wording such as "Closed Area" and "Keep Out".

When considering the use of concrete barricades, it is important to take note of adjacent perimeter control. A vehicle can easily circumvent barricades by driving through an adjacent chain link fence instead.

Potential Down-side: Depending on the number of concrete barricades used, their manufacture, and the way they are configured, it is possible to defeat them with a large powerful vehicle. To be most effective, barricades should be made of concrete over a large rebar frame, and installed in an overlapping pattern to sequentially slow, then stop, any approaching vehicle. Concrete barricades cannot be quickly positioned. It can take up to 30 minutes to re-position five concrete barricades a short distance.

Conclusion: Concrete barricades are an inexpensive means to provide high level anti-vehicle barricade security.

Cost: USD 80-100 per eight-foot concrete barricade.

Best Practice: Barbed Wire Placed Along Bottom of Fence Line

Category:	Perimeter Control
Location:	Port of Bontang, Indonesia
Date Observed:	21 June 2006
PoC:	John Szot Email: JohnSzot@badaking.co.id

Description: Barbed wire placed at strategic locations along the base of a fence line.

Discussion: Barbed wire is commonly integrated onto the tops of fence lines to deter scaling. Installation of barbed wire along the bottom of the fence line can deter efforts to gain access underneath the fence or act as an additional deterrent to fence climbing.

Potential Down-side: Additional maintenance and installation costs.

Conclusion: Barbed wire is a cost-effective way to improve security of perimeter fencing.

Cost: USD 10-40 per foot of fencing.

VIII. Security Infrastructure

Best Practice: Security Implementation Cost Recovery

Category:	Security Infrastructure
Location:	CentrePort Wellington, New Zealand
Date Observed:	29 September 2004
PoC:	CentrePort, Security Tel: +64 4 495 3829
Website:	www.centreport.co.nz

Description: CentrePort has begun to levy an NZD 300 flat fee security surcharge for all ships that use their facilities. The fee is to allow the port to recuperate their costs of installing, retrofitting, and maintaining new security measures to ensure their compliance with the ISPS Code.

Discussion: A security levy or surcharge can be done at any port or facility. Depending on local law, regulation, or ordinance, facility operators will need to provide a time frame of advance notice to shippers regarding the fee implementation and dates. After the implementation date, fees will be imposed on all ships using the port. Fees can be fixed (as above) or scaled to the tonnage or length of each ship.

Potential Down-side: A security surcharge may discourage some shippers from using a particular port or facility, especially if nearby ports or facilities do not impose similar security levies. Any new fees, levies, or surcharges increase the costs to shippers, resulting in higher shipping costs for exporters.

Conclusion: A security levy or surcharge is a low cost, high rate-of-return best practice. A security surcharge of a few hundred dollars is relatively inexpensive when compared to other shipping/docking costs. Companies can write off the expense or increase shipping fees as a cost of doing business.

Cost: Administrative costs to research and implement the security surcharge and to manage the funds received as a result of the surcharge.

Best Practice: Daily Port Security Status Report

Category:	Security Infrastructure
Location:	Port of Brisbane, Australia
Date Observed:	10 October 2004
PoC:	Mr. Les Wallace

Description: A port watch daily task planning document.

Discussion: The port security status report covers a 24-hour period and includes facility status reports, security patrol requirements, and general port information. All security personnel are required to read and initial it prior to the beginning their shift. Documents of this type can also include updated information regarding the name of the duty person in charge, specialized security equipment that is out of service, ships in port, weather forecasts, emergency phone numbers, tide tables, safety updates, lookouts for suspicious persons or vehicles, etc.

Potential Down-side: None.

Conclusion: The port watch daily task planning document is an effective way of passing critical information to the security personnel at a port. The port facility security officer enters critical information for the port on a daily basis.

Cost: The time it takes for one employee to prepare and disseminate the document.

Best Practice: Scale Diorama of Port Area

Category: Security Infrastructure

Location: Port of Neva Sheva Mumbai, India

Date Observed: May 2005

Description: The port built and maintains a scale diorama of their port in the port headquarters. The diorama can be used to plan emergency preparedness and response and for effective tabletop security exercises.

Discussion: A scale diorama of a port and access roads is a very effective tool for security planning, response, training, and exercises. Port directors and security managers can devise more realistic security threat and response scenarios during training and exercises. During an actual security event, incident commanders can coordinate the response of security officers, port employees, law enforcement, and military personnel to various locations on the port. A port diorama can provide additional benefits to a port, including safety planning, vessel and vehicle routing, and improving operational efficiency.

Potential Down-side: Port directors and security managers should not become overly reliant on table-top exercises as they do not address all of the issues that will occur during an actual security incident. It is important to hold both table-top and facility-wide practical security exercises to be best prepared for an actual security incident. Dioramas need to be updated to reflect actual port conditions as port facilities are added or removed.

Conclusion: A diorama of a port facility can provide the port with several benefits, including effective security planning, training, and incident response. Most medium and large ports would derive a benefit from constructing a port diorama reflecting all entrances, exits, fences, gates, and waterfront facilities.

Cost: Varies, depending on the size of the port, the size and amount of detail of the diorama, as well as if it is professionally built or constructed in-house. Prices will range between USD 250-10,000 to construct.

Best Practice: Dive Inspections of Ship's Hull

Category:	Security Infrastructure
Location:	Various Ports throughout Jamaica (Montego Bay pictured)
Date Observed:	April 2005
PoC:	Mr. Nicholas Baylis Ms. Beverley Stewart Port Authority of Jamaica Email: nbaylis@portjam.com bstewart@portjam.com

Description: 90 – 100% of ship hulls are inspected by divers prior to vessel movement.

Discussion: Many port facilities have employed divers to inspect ship hulls and facility piers as a counter-drug trafficking effort, as traffickers seek to utilize parasitic devices to smuggle drugs. Suspicious and dangerous items, including limpet mines, improvised explosive devices, or other weapons packaged for shipment in magnetic containers pose a threat to ships and port infrastructure. If underwater cameras to remotely assess ship's hulls are not feasible, then divers should be considered. Private contract divers can be hired to perform this service, or employees can be trained to perform this mission.

Potential Down-side: Water conditions, including environmental hazards and water clarity may hamper the effectiveness of divers. The cost of training and equipping, as well as the personal safety of divers undertaking hull inspections, and possible challenges to their integrity should be considered. Criminal or terrorist organizations may seek to bribe divers or other security inspectors.

Conclusion: Using divers to inspect ship's hulls can reveal a number of security, safety, and other important issues. Instituting cooperative policies between military or law enforcement divers and port facilities can resolve many of the potential concerns involved with this security practice. Security is only as good as its weakest link and often underwater searching and monitoring of ship hulls is neglected.

Cost: Varies; approximately USD 200 per hull assessment using one diver.

Best Practice: Electronic Mooring System

Category:	Security Infrastructure
Location:	Port of Bontang, Indonesia
Date Observed:	21 June 2006
PoC:	John Mclellan John_m@banpuindo.co.id

Description: Electronic mooring system continuously measures and updates the approach speed of incoming ships during mooring evolutions.

Discussion: This system uses two laser sensors that measure distance to the bow and stern sections of the ship. This, together with average speed, is captured at the jetty control unit and displayed to the ship and mooring crew on a wireless monitor, computer screen or jetty mounted display board, as required. The system of red and green indicating lights, with green indicating that approach speed is within the 10cm/second tolerance for post Panamax size vessels and red indicating the speed is too great, allows for suitable speed adjustments to be made. While not necessarily providing a security element, this system helps to ensure the safety of the facility.

Potential Down-side: The cost may be prohibitive for many facilities.

Conclusion: For facilities that can afford this technology, the ability to provide real-time feedback of a ship's position during mooring evolutions can help reduce accidents and minimize damage to ships and the facility.

Cost: USD 40,000-100,000.

Best Practice: Area Maritime Security Committees

Category:	Security Infrastructure
Location:	Each major U.S. port area
Date Observed:	2002
PoC:	Captain of the Port
Website:	Area Maritime Security Committee

Description: The Area Maritime Security Committee (AMSC) is a collaborative forum where government and industry partners work together to enhance security in the maritime environment. Established under the Maritime Transportation Security Act of 2002, the AMSC focuses on maritime security, including contingency planning, developing security plans, and fostering communication between port stakeholders.

Discussion: Each Committee conducts an Area Maritime Security (AMS) Assessment, maintains an AMS Plan, and conducts AMS training and exercise programs. The AMS Committee meets regularly, typically four times a calendar year, when requested by the COTP (a.k.a. Sector Commander), or when requested by a majority of AMS Committee members. Key components of AMSC responsibilities:

- Identify critical port infrastructure and operations
- Identify risks (threats, vulnerabilities, and consequences)
- Determine mitigation strategies & implementation methods
- Develop and describe the process to continually evaluate overall port security
- Provide advice to and assist the COTP in developing the AMS Plan

Potential Down-side: Dedicated time commitment.

Conclusion: This best practice includes many components of the ISPS Code (e.g. Communication, Cyber, Documents & Forms, Training & Procedures, etc.), optimizing regional port security coordination.

Cost: There is no cost for membership.

Best Practice: Centralised Parking Plaza

Category:	Security Infrastructure
Location:	Jawaharlal Nehru Port Authority, Nhava Sheva
Date Observed:	October 2021
Website:	www.jnport.gov.in

Description: Implementation of centralised parking plaza for efficient, safe, and secure cargo movement.

Discussion: The plaza has been built exclusively to integrate the parking of tractor trailers carrying factory stuffed export containers at one location instead of multiple locations earlier. This will help integrate document processing by Customs with state-of-the art facilities and service provision. JNPA is the only port in India which has planned for a facility of this scale and is a key initiative to streamline the traffic movement and improve the port efficiencies using IT services, while at the same time providing convenience facilities and amenities at very nominal rates to truck drivers who travel long distances to reach the port.

Conclusion: This facility helped to reduce the dwell time of export containers and streamline the flow of trucks. This has tremendously reduced the risk of intrusion of unauthorized persons and trucks into the port area.

IX. Training and Procedures

Best Practice: Port Security Officer for Ports and Managing Drills and Exercises

PNG PORTS

MEMORANDUM

From: Security Manager To: All PSO's/PFSO's, All Port Managers

Ref: 026-PSM-07/MP Date: 15/04/07

Subject: ISPS SECURITY DRILLS & EXERCISES SCHEDULE FOR 2007

It is an ISPS requirement that we test our approved Port Security Plans by way of conducting Security Drills & Exercises every three months to test our security systems and response capacities in individual ports in consultation with our civil emergency organizations and stakeholders.

Below is a schedule for the remainder of 2007 to assist Port Facility Security Officers plan and

Category:	Security Infrastructure
Location:	PNG Ports Corporation Ltd. Papua New Guinea
Date Observed:	May 2007
PoC:	Michael Piel Port Security Officer PNG Ports Corporation Ltd.

Description: PNG Ports Corporation hired a Port Security Officer (PSO) to oversee security at all its facilities. All Port Facility Security Officers (PFSO) report to the PSO, as well as their own facility management. Additionally, the PSO developed a master schedule to ensure that all facilities carry out their drills and exercises.

Discussion: The PSO provides a senior level technical expert for PFSOs to help them meet their policy and budget needs. This overarching corporate security organization creates efficiencies in standardized training, policies, and equipment purchases. It also allows for company oversight and assistance to individual facilities in the conduct of required drills and exercises. The PSO serves as a resource to help facilities plan and execute their drills and exercises.

Potential Down-side: It requires a position dedicated solely to security.

Conclusion: PNG Ports Corporation created this position because it made business sense. They have significantly reduced theft and loss of cargo as a result of this position and created an effective drills and exercise program.

Cost: The cost of hiring a full-time security professional/manager. However, PNG Ports Corporation has realized savings as a result of loss prevention and efficiencies realized through standardization.

X. Other Best Practices

Best Practice: Establishing the Maritime Security Transit Corridor and Mandatory Reporting Area in Sulu-Celebes Sea

Category:	Other Best Practices
Location:	Sulu and Celebes Sea Philippines
Date Observed:	2004
PoC:	Philippine Coast Guard
Website:	https://coastguard.gov.ph

Description: The Maritime Security Transit Corridor was established in Moro Gulf and Basilan Strait to prevent or suppress acts of piracy and armed robbery transiting Sulu and Celebes Seas.

Discussion: All vessels navigating Moro Gulf and Basilan Strait, except government vessels engaged in maritime law enforcement, must adhere to the designated transit corridor. Unlike a traffic separation scheme, it aims to enhance monitoring by the Philippine Coast Guard (PCG) and other law enforcement units in the area. With clearly defined transit areas, vessels can be closely observed, and law enforcement units are strategically positioned nearby to maintain a heightened awareness of the operational environment.

Reporting Area in Sulu-Celebes Sea (ReCAAP) reported no piracy incidents in the Sulu-Celebes Seas in 2023, with the latest recorded on 17 January 2020. Under the current program, the perceived incapacity of perpetrators to execute attacks within the transit corridor suggests that incidents are improbable. Nonetheless, in the event of potential attacks, only minimal damage to the ship and crew may be expected.

Potential Down-side: Dedicated patrol vessels should be stationed near the transit corridor to ensure swift response capabilities if needed.

Conclusion: All vessels in Moro Gulf and Basilan Strait, except government ones enforcing maritime law, must adhere to the transit corridor. Unlike a traffic separation scheme, it aims to enhance monitoring by the PCG and other law enforcement units. No piracy incidents were reported in the Sulu-Celebes Seas in 2023, with the latest recorded on 17 January 2020. Despite the perceived reduced threat, patrol vessels remain stationed nearby for quick response if needed.

Cost: Relatively low as regular maritime patrol activities are inherent to the PCG's duties.

Best Practice: Collaborative efforts on Unmanned Technology

Category: Other Best Practices
Location: United States of America
Date Observed: 2023

Description: U.S. port partners collaborating on understanding quickly evolving unmanned aerial, surface, and subsurface technology.

Discussion: Unmanned systems is a reoccurring focus of the U.S. Coast Guard Area Maritime Security Committees. Port partners work in subcommittee to integrate technology into maritime security operations, identify origination of unmanned aerial system conducting unauthorized flights over vessels, and testing remote sensor technology to detect unmanned surface vessels.

Potential Down-side: Port partner collaboration adds additional workload to staff members and requires members to invest time and resources learning about the technology and capabilities of unmanned systems.

Conclusion: Unmanned aerial, surface and subsurface technology continues to evolve such that maritime security professionals, and the maritime industry must continuously understand current system capabilities and incorporate into threat assessments against critical infrastructure and key resources. Information on system capabilities from just a few years ago is quickly outdated and reliance may yield a false sense of security regarding protective measures.

Cost: Unknown.

Best Practice: Market Denial Operations

Category:	Other Best Practices
Location:	Port of Manila Philippines
Date Observed:	2004
PoC:	Philippine Coast Guard
Website:	https://coastguard.gov.ph

Description: Market denial operations aim to reduce the financial incentives driving maritime crime.

Discussion: As maritime threats evolve, the Philippine Coast Guard (PCG) employs a proactive 'market denial' approach to combat the illicit trade of stolen goods from ships. This strategy aims to disrupt the entire illicit supply chain by obstructing avenues through which stolen goods are traded and sold. By intercepting and confiscating illicit cargo, PCG not only thwarts immediate profits for criminal enterprises but also dismantles their long-term viability.

Furthermore, 'market denial' serves as a potent deterrent against engaging in such illegal activities. By depriving perpetrators of the opportunity to profit from their gains, PCG reduces the financial incentives driving maritime crime, thereby diminishing motivation for further unlawful behavior. By targeting both the market and criminal networks, the PCG ensures the protection of maritime commerce and upholds the rule of law, contributing to broader efforts in maintaining security and stability in the region.

Potential Down-side: Other port regulators may not have law enforcement powers, but they can reach out to other government agencies in their country who can complement the port authorities.

Conclusion: The PCG uses a 'market denial' strategy to combat maritime threats by disrupting the illicit trade of stolen goods from ships. This approach aims to obstruct avenues used by criminals, reducing financial incentives for maritime crime, and contributing to broader security efforts in the region.

Cost: Relatively low as regular law enforcement activities are inherent to the Philippine Coast Guard's duties.

Best Practice: Implementation of the ISPS Code in China

Category:	Other Best Practices
Location:	Not applicable
Date Observed:	Not applicable
PoC:	Not applicable

Description: The International Ship and Port Facility Security (ISPS) Code, adopted under the SOLAS Convention, establishes a systematic security management framework for global maritime safety. China has implemented the ISPS Code through a comprehensive approach, integrating legal, technological, and operational measures to enhance ship and port facility security.

Discussion: 1) Legal Framework: China has developed a robust legal system aligned with the ISPS Code, including the Maritime Traffic Safety Law, Port Facility Security Rules, and International Ship Security Rules. These laws mandate security assessments, plan approvals, and certification processes.

2) Technological Integration: China employs advanced technologies such as AIS base stations, VTS centers, LRIT systems, and UAVs for real-time monitoring and risk alerts, forming a "land-sea-air-space" security network.

3) Inspection and Compliance: China conducts over 7,000 Port State Control (PSC) inspections annually, with a focus on ISPS Code compliance. Inspection efficiency and deficiency detection rates have significantly improved, setting a benchmark in the Asia-Pacific region.

4) International Collaboration: China actively participates in global maritime security initiatives, including ReCAAP and joint counter-piracy operations, contributing to regional and international maritime safety.

Potential Down-side: 1) High Initial Costs: Implementing advanced technologies (e.g., UAVs, smart monitoring systems) requires significant investment in equipment and training.

2) Regulatory Complexity: Strict compliance with evolving international and domestic regulations may pose challenges for smaller facilities.

3) Coordination Requirements: Effective implementation demands seamless collaboration between multiple agencies and stakeholders.

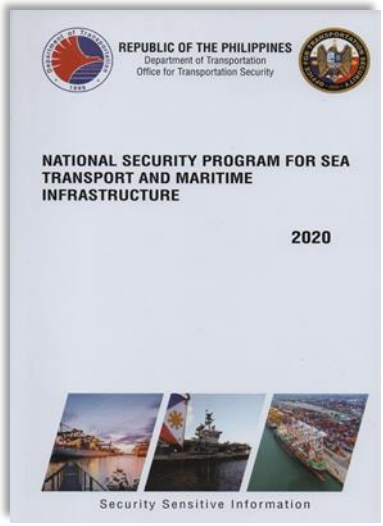
Conclusion: China's implementation of the ISPS Code demonstrates a holistic approach combining legal rigor, technological innovation, and international cooperation. While the initial costs and coordination efforts are substantial, the long-term benefits in security enhancement and global compliance are undeniable. Regional variations may require tailored adaptations, but China's model offers valuable insights for maritime security governance worldwide.

Cost: 1) Initial Costs: Procurement of security equipment (e.g., AIS, VTS, UAVs) and system installation.

2) Training Costs: Regular drills and certification programs for security personnel.

3) Ongoing Costs: Maintenance, upgrades, and compliance audits to ensure sustained effectiveness.

Best Practice: Promulgation of the National Security Program for Sea Transport and Maritime Infrastructure



Category:	Other Best Practices
Location:	Philippines
Date Observed:	27 February 2020
PoC:	Jose A. Briones, Jr. Officer-in-Charge Office for Transportation Security
Website:	www.ots.gov.ph

Description:

The National Security Program for Sea Transport and Maritime Infrastructure (NSPSTMI) is

- A transposition of Chapter XI/2 and ISPS Code to safeguard maritime transportation in the Philippines against unlawful interference and acts of terrorism.
- A manual prescribing maritime security standards, policies, and procedures and responsibilities of other government agencies, and kept under constant review to adjust relevant elements based on a security risk assessment carried out by relevant national authorities.
- Signed by the Secretary of the Department of Transportation.

Discussion:

The Philippines promulgated NSPSTMI on 7 February 2007. The 2007 edition of the NSPSTMI consists of Book I (International) and Book II (Domestic). However, the Philippines is bound to embrace the Code as the country's own legislation, under the Convention, by virtue of the constitutionally enshrined doctrine of incorporation and principle of state responsibility. Thus, in 2020, a revised NSPSTMI was issued to establish and implement maritime security policies and procedures and shall be kept under constant review to adjust relevant elements based on a security risk assessment carried out by relevant national authorities, to safeguard and protect domestic maritime transportation from acts of terrorism or unlawful interference. This program focuses on prescribing standard security measures and procedures for domestic maritime transportation only, to safeguard and protect it from acts of terrorism or unlawful acts, and to ensure that these standard security measures and procedures are in place on board Philippine ships and on port facilities. The revised NSPSTMI integrates relevant executive issuances and provides for the following:

- Responsibilities of the SOTr;
- Broader responsibilities of OTS, which include, among others, the

accreditation of maritime training institutions and certification of maritime security personnel;
- Inclusion of National Coast Watch Center as the intelligence fusion center for maritime security operations;
- Definition for acts of terrorism, audit, Declaration of Security (DoS), drills, exercise, maritime security auditor, Registered Security Organization (ReSO), and unlawful acts;
- Wider coverage of the Program, to include cargo ships with 150 GT and tugboats;
- Non-limitation on the GT for cargo ships carrying dangerous substances;
- Qualifications and duties of ship/port owner/operator, CSO, SSO/PFSO, shipboard personnel, port facility personnel, with or without security duties, and port facility service providers;
- Additional sections for documentation; training, drills and exercise; physical security measures; operational security measures; and incident response;
- Exclusion of security regulated ports; and
- Enforcement measures for compliance of maritime sector.

Potential Down-side: While the NSPSTMI was promulgated to secure the port facilities and ships engaged in domestic voyages and involves cooperative enforcement between and among government agencies under DoTR, it has also potential down-sides that can possibly affect attaining the objective of the program, such as:
- Lack of cooperation/support of other agencies for cooperative enforcement;
- Training capability of other government agencies for ISPS and other maritime regulations; and
- No administrative fines, penalties, or sanctions imposed for the port facilities and ships found to be non-compliant to the provisions of the NSPSTMI and the ISPS Code.

Conclusion: The OTS, as Designated Authority and Administration of the ISPS Code in the Philippines has been in constant coordination with other government agencies, engaging through cooperative enforcement via a memorandum of agreement (MOA) to concerned agencies with maritime security mandates mentioned in the NSPSTMI. The agencies mentioned, among other are the following: Maritime Industry Authority (MARINA), Philippine Coast Guard (PCG), port authorities, such as: Philippine Ports Authority (PPA), Cebu Port Authority (CPA), Subic Bay Metropolitan Authority (SBMA), Bangsamoro Port Management Authority (BPMA) and PHIVIDEC. As of date, CPA, SBMA, BPMA and PHIVIDEC have agreed to execute a MOA with the OTS. Meanwhile, PPA and the LGU have issued a Department Order in support of the mandate of OTS regarding requirement of the IMO to enhance maritime security. Despite the potential downside of the NSPSTMI implementation, the OTS is determined, by all means, to continue its effective compliance monitoring of port facilities and ships to the ISPS Code,

including OTS partnership with other foreign counterparts such as: United States Coast Guard and the United Kingdom Department for Transport. The mandate of OTS as Designated Authority and Administration to implement the ISPS Code is well-defined in the IMO Security Needs Assessment Mission report conducted in 24-28 February 2020, Manila, Philippines.

Cost:

The promulgation of the NSPSTMI has incurred minimal expenses, limited to research, consultative meetings with the stakeholders and agencies of the government with maritime security-related mandates, and printing of the document itself for distribution.

Best Practice: Creation of Nodal Agency at Apex Level in Government

Category:	Other Best Practices
Location:	Office of National Maritime Security Coordinator, India
PoC:	Joint Secretary Maritime Security Email: js-msip@gov.in

Description: Creation of a nodal agency at the apex level in the Government of India towards ensuring coordination between all cross-functional stakeholders concerned with port security.

Discussion: India, being one of the largest maritime nations in the world with a coastline of more than 11,000 km, has more than 200 ports across nine Coastal States and four Union Territories of the nation. Apart from these 200-plus ports, there are several single point moorings which enable the transfer of oil to shore infrastructure. The all-encompassing security of all these assets involves multiple cross-functional stakeholders at the central and state government levels. These stakeholders include Navy, Coast Guard, Marine Police, Port Authorities, Maritime Boards, Customs, Fisheries, Security Agencies (both government as well as private), private operators, Environmental Agencies, and others. While all these stakeholders have their regulations, orders, standard operating procedures, guidelines, etc., a need was felt to synergise the efforts of all the stakeholders on a common platform to have a holistic and comprehensive national maritime security. Towards ensuring this, the Government of India has created a multi-agency structure headed by the National Maritime Security Coordinator (NMSC) at the apex level under the Office of the Prime Minister. The NMSC ensures coordination among various stakeholders in the realm of maritime security including coastal, offshore and port security by conducting periodic review meetings to address challenges and bottlenecks, including those impacting port security. The NMSC also serves as the single point of contact to resolve inconsistencies, gaps, and redundancies in the various orders issued by the stakeholders. The Office of NMSC also issues periodic publications in the form of issue-briefs, reports, newsletters, acquaints, etc. for seamless alignment and collective synergy among the stakeholders. In addition, an electronic/digital dashboard has been created to ensure effective and timely sharing of orders and guidelines, etc. issued by maritime stakeholders.

Potential Down-side: There is no potential downside: the creation of a structure at the apex-level has ensured coherence and synergy among the maritime stakeholders to ensure comprehensive maritime security.

Conclusion:	Countries could examine the possibility of establishing linkages with a central node or point of contact at the Office of NMSC for exchanging best practices in port and maritime security. This could be established at an equivalent apex level in the respective ARF participant governments to deal with maritime security aspects.
Cost:	No cost implications.

Best Practice: Implementation of ISPS Code on Indian Coastal Vessels Including Vessels Less than 500 GT

Category:	Other Best Practices
Location:	Location: DG Shipping - Indian Flag Vessels
Date Observed:	2004
PoC:	Nautical Adviser to the Government of India Email: na-dgs@nic.in
Website:	www.dgshipping.gov.in/index.aspx

Description:

SOLAS XI-2/2/1.1 mandates ISPS Code applicability to all vessels – MODUs, passenger ships (including HSCs), and cargo ships (including HSCs) 500 GT and above – engaged in international voyages.

However, keeping security paramount, since the implementation of the ISPS Code in India—i.e. since 2004—India has mandated that Indian coastal vessels, including vessels less than 500 GT, must also comply with the ISPS Code requirements, as outlined in applicable administrative orders. The and same is now being implemented through Merchant Ship (Ship and Port Facility Security) Rules, 2024. This enhances India's security in coastal waters and enhances maritime domain awareness to ensure safe and secure seas.

Discussion:

India's decision to implement ISPS Code on coastal vessels and cargo vessels less than 500 GT enhances India's maritime security, as it encompasses smaller and coastal vessels which at times pass through the security net undetected. Further, these small vessels may be used for illegal trade and benefits, hence bringing them under security umbrella (ISPS). These measures address threats from such vessels and trade, thereby enhancing security in Indian waters.

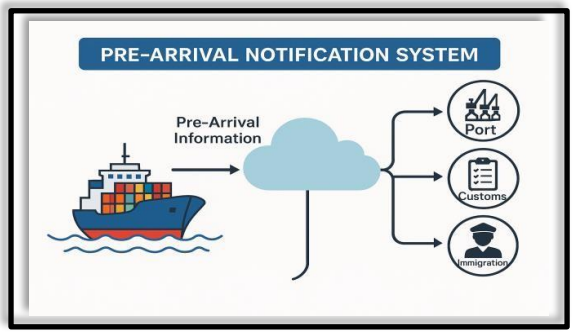
Specific ISPS requirements for coastal vessels and vessels less than 500 GTvary depending upon the size of the vessels, however these include having a Ship Security Plan, appointing a Ship Security Officer and Company Security Officer, installing a Ship Security Alert System, having the required security equipment, conduct of periodic audits, etc. These additional security measures strengthen coastal surveillance, enhance situational awareness of port and naval authorities, and foster a disciplined security culture, aligning with India's 'MAHASAGAR' (Mutual and Holistic Advancement for Security and Growth Across Regions) vision. It also accelerates port entry vetting and positions small vessel operators as vital partners in national security, appealing to facility managers and security officers for improved operational readiness.

Potential Down-side: Only downside is the added cost due to incorporating additional ISPS requirements, which are not mandatory as per the SOLAS XI- 2 or the ISPS Code. These additional costs not only include the additional required equipment, but also additional manpower for effective implementation and administration of the ISPS Code.

Conclusion: India's voluntary extension of the ISPS Code to its coastal vessels, and cargo vessels under 500 GT, adds to the operational cost of Indian shipping but significantly enhances maritime security and maritime domain awareness in Indian waters. Hence, the cost-benefit analysis weights favorably towards this best practice. Further, implementation of this best practice for the last 20+ years is testimony of the statement.

Cost: The cost varies, as it includes additional equipment, manpower, audits, etc., depending upon the size of the vessel. However, these are not substantial in nature.

Best Practice: Implementation of Pre-Arrival Notification System for Yachts



Category:	Other Best Practices
Location:	DG Shipping – Yachts India
Date Observed:	5 February 2020
PoC:	Nautical Adviser to the Government of India Email: na-dgs@nic.in
Website:	www.dgshipping.gov.in/index.aspx

Description: As per the ISPS Code, SOLAS XI-2/9/2 requires all vessels intending to enter a port of another Government to provide information requested by the concerned port. India implemented these requirements vide administrative circulars issued by DG Shipping in 2005 and 2014.

However, these requirement did not cover the Yachts and Mechanized Sailing Vessels (MSVs), therefore under administrative orders issued in 2020 and 2017, pre-arrival notification was made mandatory for Yachts in 2020 and for MSVs under specific instructions issued in 2017.

Discussion: India's decision to bring Yachts and MSVs under the Pre-Arrival Notification System (PANS) not only enhances maritime security and domain awareness, but also enhances the safety of such vessels and their crews. The sailing plan and position reports of PANS ensure adequate information is available in case such vessels require any assistance.

Additionally, such vessels are now required to have effective communication from vessel to shore, or adequate communication arrangement through the owners especially in case of MSVs.

Potential Down-side: Only downside and challenge to this requirement is that these vessels may not have the required communication equipment to enable periodic position reporting. As discussed, this requirement enables such vessels to have effective means of communication from vessel to shore, which not only enhances maritime security and domain awareness but also safety of such vessels and its crew.

Conclusion: India's requirement of covering Yachts and MSVs under the ambit of PANS, even though the requirement may be seen as onerous on such vessels, enables them to have means of effective communication from vessel to shore, thereby not only enhancing maritime security and domain awareness but also enhancing safety of such vessels and its crew.

Cost:	The cost varies, as it would depend upon the type of communication equipment opted for by the owner or an effective communication arrangement through the owner.

Best Practice: Implementation of ISPS Code to All Port Facilities

Category:	Other Best Practices
Location:	DG Shipping – Ports India
Date Observed:	19 June 2024
PoC:	Nautical Adviser to the Government of India Email: na-dgs@nic.in
Website:	www.dgshipping.gov.in/index.aspx

Description:

It is to be noted that SOLAS XI-2/2/1.2 mandates ISPS Code applicability to all Ports serving ships engaged on international voyages, and SOLAS XI-2/2/2 allows the applicability of ISPS Code also to Ports which occasionally serve ships engaged on international voyages.

However, India under Merchant Ship (Ship and Port Facility Security) Rules, 2024, issued on 19 June 2024, has mandated ISPS Code requirements to all ports including those that serve only coastal vessels (non EXIM Ports). This measure significantly enhances India's security not only in ports but also in its coastal waters.

Discussion:

India's decision to implement ISPS Code to all ports including the ones which do not serve ships on international voyages, enhances India's maritime security, as it now brings an additional 240 ports under ISPS domain that previously were not required to be ISPS compliant, thereby directly enhancing costal security and domain awareness on the entire Indian coast. Furthermore, including these additional ports under ISPS develops the interface between Central Authorities and the respective State Authorities that previously were solely responsible for the security of such ports.

India's maritime security is elevated by this inclusive and forward looking approach, protecting its vast port ecosystem from terrorism, smuggling, and unauthorized access. By standardizing procedures across all facilities, it enables coordinated response, situational awareness, and operational efficiency, surpassing global norms that focus only on EXIM ports. This aligns with the 12 June 2025, meeting's strategic intent, supporting India's 'MAHASAGAR' (Mutual and Holistic Advancement for Security and Growth Across Regions) vision with shared technologies and joint exercises, appealing to managers for secure and efficient logistics.

Potential Down-side: Only downside is the added cost due to incorporating additional ISPS requirements, which were not mandatory earlier. This additional cost includes equipment, competent manpower, and administration of the ports' ISPS certification. This cost would be significant in nature and would differ from port to port depending upon its size and handling capacity and would be borne by the State Government and the operator of the port.

Conclusion: India's voluntary extension of the ISPS Code to all its Ports including those which serve only coastal vessels (non-EXIM ports) would increase cost of port operations, would be borne by port operators, and would be applicable to all ports ensuring uniformity. Further, the benefit the country attains by way of increased security in Indian waters, easily offsets the additional cost.

Cost: The cost would vary from one port to another and would depend upon its size, handling capacity, and nature of cargo being handled.

ASEAN REGIONAL FORUM

Promoting peace and security through dialogue and cooperation in the Asia Pacific