The proposed tiers of using ISO 20858:2007 in port facilities

MAGED MOHAMED ALY HASSABOU

Head of Consultancy Department, Regional Maritime Security Institute, AASTMT

MOHAMED MAHMOUD ABDEL FATTAH

Head of Training Department, Regional Maritime Security Institute, AASTMT

Abstract

The port facilities' compliance with the international ship and port facility security code (ISPS Code) and other international requirements is verified through periodical verifications and reviews carried out by administrations as well as port facilities' operators. These verifications mainly focus on the documentary requirements of the ISPS Code and pay just little attention to the practical aspects of port facility security plan (PFSP) implementation (Teck& Shah,2008).

In addition, the periodical verifications and reviews are not considered as a clear evidence for port facilities' compliance for the international requirements. Moreover, this is against the spirit of the ISPS code and usage of PFSPs as proactive procedures and measures that could provide instructions for the executing plans in port facilities capable to provide guidance and references in implementing of the security procedures and measures.

having a Statement of Compliance for Port Facility (SoCPF) is not a clear or physical evidence for a port facility to prove its fully compliance with the necessary requirements of the ISPS code and the other mandatory international requirements. The aim of this paper is to offer an instrument tool for port facilities to ensure executing and complying with maritime security requirements. Also, it proposes three tiers for using ISO 20858 to accomplish the aim of the paper and recommends using such tiers in Egyptian port facilities.

***Keywords*:** ISO 20858, maritime security, Port Facility Security Plan, ISPS Code.

1. Introduction

The impact of 9/11 has caused a considerable change in the role of International Maritime Organization (IMO) in dealing with maritime issues from just focusing on “Safer Shipping and Cleaner Oceans” to “Safe, Secure and Efficient Shipping on Clean Oceans” (Gunasekaran,2012). The reformation towards security issues by the IMO reflects its broader and deeper interest in offering a blueprint for better response in the future (IMO, 2010) which eventually caused a positive change of attitude in the international maritime industry stakeholders with the involvement and co-operation of other international organizations such as international labor organization (ILO),world custom organization (WCO) and International Organization for Standardization (ISO) without denying that the influence of some countries either directly or indirectly through these organizations is equally important.

IMO, WCO & ILO issue regulations and requirements. ISO, as a linking instrument, transform those regulations and requirements into industry standards. Then, industry standards are provided to be voluntary complied in shipyards, shippers, transporters, ship owners and operators, terminals and port facilities by regulatory bodies as recognized security organizations (RSOs) (Li, 2011).

The ISPS Code is one of the fastest implemented regulations in the entire history of IMO. It took just 18 months from the approval of the amendment to safety of life at sea convention (SOLAS 74) until it entered into force (UNCTAD, 2013). even though, such fast implementation has both advantages and disadvantages; the main advantages of the enforcement of the ISPS code are that maximized the control of access to port facilities and onboard ships. It has also minimized theft and sabotage in port facilities and onboard ships. These advantages offered by the ISPS Code are very important elements to identify risks. Risk identification is very crucial to ensure that the maritime security risk management system functions well.

In addition to the ISPS Code, the Code of Practice on Security in Ports was developed as a result of cooperation between both the IMO and ILO. The guidelines offered by this Code covered a more defined framework for many aspects in the security of port facilities. The risk assessment of port facilities is given a special concern in this Code where The full methodology suggested go beyond the ISPS Code requirements (Gunasekaran, 2012). This was followed by some other subsequent initiatives such as the ISO Standards like ISO 20858, providing guidelines on maritime port facility security assessment, demanding that the relevant port authority develop a port facility security plan and ensure its application in the case of the critical port facility assets, ISO 28000, providing guidelines on security management supply chains (Bichou, Bell and Evans,2014).

Failure to such comply with the international maritime security requirements would result in failure to obtain national and international recognitions that could lead to degrade commercial competitiveness of those ports which presents the main problem for this paper. consequently, the shipping companies, shippers and freight forwarders could switch to other compliance ports.

2. (ISO) standard regarding to maritime security

Ports are considered as hubs for the international trade, therefor they shall be operated efficiently and effectively. This concept shall be completely applied on port security processes and operations. While laws and regulations mandate certain security standards, total quality management (TQM) and other quality standards. The quality standards such as ISO certification criteria require specific improvements in processes to enhance productivity and profitability of port operations. Security is a critical issue of each of these elements. For that reason, this section of paper briefly displays ISO standards regarding to maritime security (Abdel Fattah,2015).

ISO has issued many of maritime and supply chain standards that are replacing the originally published Publicly Available Specifications (PAS) documents such as ISO 28000 and ISO 20858.

2.1. ISO (28000:2007): It specifies the requirements for a security management system, including those aspects that are critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. These aspects include all activities controlled and influenced by organizations that have an impact on supply chain security. Other aspects should be considered directly, where and when they have an impact on security management, including transporting the cargoes along the supply chain. ISO (28000:2007) is applicable to all sizes of organizations, from small to multinational in manufacturing, service, storage or transportation at any stage of the supply chain (UNCTAD, 2016).

2.2. ISO (20858:2007): It establishes a framework to assist marine port facilities in specifying the necessary competence of personnel to conduct a marine port facility security assessment and to develop a security plan as required by the ISPS Code. ISO (20858:2007) assists marine port facilities in conducting the marine port facility security assessment, and drafting or implementing a port facility security plan (PFSP). In addition, ISO (20858:2007) establishes certain documentation requirements designed to ensure that the process used in performing the responsibilities and duties described above were recorded in a manner that would allow independent verification by a qualified and authorized agency if the port facility has agreed to such review (UNCTAD, 2016).

2.3. ISO (27000 series): These standards have been specifically reserved by ISO for information security issues. Finally, all these ISO Standards listed above, align with a number of other topics, including ISO (9001) (quality management) and ISO (14001) (environmental management) (Abdel Fattah,2015).

3. ISO (20858:2007) requirements, limitations and structure

After the adoption of the ISPS Code, the ISO Technical Committee ISO/TC 8 issued the ISO 20858:2007, concerning Ships and Marine Technologies –Maritime Port Facility Security Assessment and Security Plan Development. ISO 20858:2007 published in 2007. It replaces the PAS which had been previously issued on 1 July 2004, the same day the ISPS Code "entered into force", and is designed to assist in the uniform industry implementation of the ISPS Code (Chacon, 2016).

It is not an objective of ISO 20858 to set requirements for a contracting government (CG) or designated authority in designating a Recognized Security Organization (RSO), or to oblige the use of an outside service provider or other third party to conduct the marine port facility security assessment or develop security plan if the port facility personnel have the necessary expertise outlined in this specification. Ship operators and ships' masters should be informed that marine port facilities that use and apply this document meet an industry-determined level of compliance with the ISPS Code (ISO,2007).

3.1. Performance of the security assessment

The port facility that is implementing this International Standard, ISO (20858:2007), shall conduct a security assessment or depend upon existing security assessments that are valid, documented and meet the necessary requirements of this International Standard. The port facility security assessment shall consider all security threat scenarios, consequences of potential successful attacks on the port facility, and the likelihood of each security threat scenario being successful given the security procedures measures in place. Based on these considerations, a determination shall be made if additional security countermeasures are needed. The personnel who are conducting PFSA shall have the necessary experiences as required in the ISPS Code.

3.2. Security assessment procedures

A port facility security assessment provides the basis for developing the Marine Port Facility Security Plan. the methodology used in the assessment shall meet the requirements of ISO 20858. The scope of the assessment extends to those port facilities and port infrastructures that could be threatened or be used to threaten maritime trade. The port facility security assessment shall include, at least, all these areas:

- where port facility/ship operations are conducted within the port facility,
- where cargoes are staged, stowed or handled before/following marine transportation in the port facility,
- where cargoes documentations for marine transportation are handled/accessible in the port facility,
- attached to the port facility without an intervening security perimeter,
- including ship anchorage areas/ channels used to approach the port facility.

The PFSA shall include all areas interfacing between ships and port facilities. The personnel who are conducting the assessment shall review all existing security operations and contingency plans in the port facility. These personnel shall also conduct on-scene security survey in the port facility, examine and document all important operations during such assessment. The PFSA shall identify all crucial assets and infrastructure in the port facility. Besides, the personnel conducting PFSA shall communicate with and consult the local law enforcement and all other appropriate government officials responsible of securing the port facility against any potential threat. All information received shall be documented and considered (ISO,2007).

The methodology used to conduct a security assessment shall, at least, identify the security threat scenarios documented in ISO 20858. A thorough evaluation of consequences shall be conducted and carefully consider potential the loss of lives, economic losses and environmental pollution. The consequences of each security incident evaluated at a port facility shall be classified as high, medium, or low. In case of using the numerical system in the security assessment process, the numerical results shall be converted into a qualitative system. Rationales for the classifications of consequences for each security incident shall be documented. The values of “high”, “medium”

and “low” consequences shall be thoroughly determined. The likelihood of each security scenarios becoming a security incident should be classified as high, medium and low (ISO,2007).

The rationale for the classification of likelihood that is assigned to every security scenario shall be documented. the security scenarios scoring chart shall be utilized to know exactly when countermeasures must be considered for specific security scenarios. The person who is assessing the security shall document every single security scenario required to be considered for countermeasures. When utilizing the methods specified in ISO 20858, each countermeasure shall be assessed for influence in lowering the likelihood or /and consequences until the security scenario no longer needs that countermeasures be considered. The countermeasure accomplishing this is considered to be efficient and shall be documented in the PFSP. Figure.1 Evaluating the security process (ISO Focus ,2006).

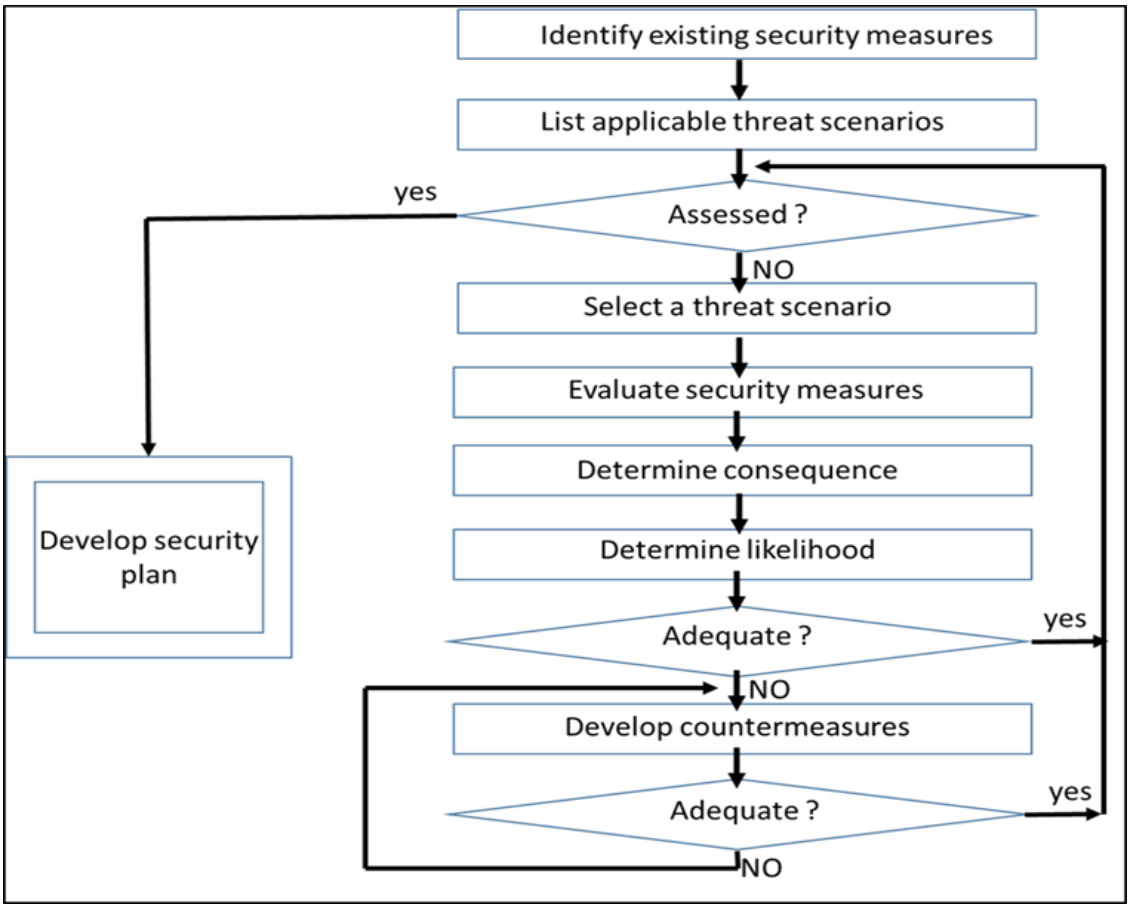

Figure.1 Evaluating the security process. Source: ISO Focus ,2006

3.3. Port Facility Security Plan (PFSP)

A PFSP shall be developed to ensure the implementation of measures assigned to secure the personnel, port facility, ships, cargoes, cargo transport units and ships’ stores in the port facility against all potential risks of any security incident. The countermeasures shall be implemented, in

such order, to maximize benefits as assessed unless the CGs set other concepts. Countermeasures determined to be implemented shall be incorporated into the PFSP in the appropriate section (ISO,2007). **Contents of the port facility plan:**

- The port facility (PF) perimeters or areas covered by the PFSP are as follows:
- All exits, gates and access points, all restricted areas in the port facility including jetties, ship berths, emergency equipment, emergency shutdown controls, parking spaces, security checkpoints, vital buildings, emergency vehicle lanes, storage spaces especially for dangerous materials and all port facility assets.
- A description of the security organizational structure, including an explanation of duties and responsibilities of every person in the security organizational structure shall be documented.
- The Security organizational structural of the PF, document the name of the PFSO and all of his contact details.
- Changes in security levels and document different procedures and measures related to each security level.
- Document all security procedures and measures for interfacing with ships related to each security level.
- Document procedures for completing a Declaration of Security (DOS).
- Define the means by which the PFSO shall follow to inform PF personnel of changes in security Procedures and measures. The security system shall allow continuous effective and efficient communications among all PF security personnel, ships, the PFSO and national and local authorities that have security duties or responsibilities.
- All security systems and equipment.
- Security procedures and measures for access control, Access to restricted areas, handling cargo, delivery of ship's stores, spare parts and bunkers.
- Security incident reporting procedures.
- Any other additional requirements necessary for cruise ship, passenger and ferry port facilities.
- Periodical security audits and verifications.
- Procedures for implementing security plan amendments.
- Security training, drills and exercises.
- Security Skills, knowledge and competencies necessary of all PF personnel.
- Implementing the supply chain security plan, the organization shall establish and use an existing management system to allow all of its specific port facility security processes to be effectively and efficiently executed.

3.4. Documentation

The documents developed to meet ISO 20858 shall be maintained and secured to prevent unauthorized disclosures. Define the plans that will be used to maintain and secure all the documents listed in this clause (ISO,2007).

3.4.1. The PFSA report shall contain, at least, all of the following:

– PFSP table of contents.

– The name and location of the PF.

– The persons' names and qualifications who were conducting on-scene security survey and developing security assessment.

– The date when the PFSA was accomplished and revised.

– The date when the PFSA shall be reviewed.

– an explanation of the port facility security assessment methodology applied, including, at least, a description of the threat scenarios that were considered, the methods applied to classify consequences and likelihood, how risks were evaluated and the methods that were applied to determine the necessary countermeasures.

– The detailed maps or charts of the areas that were assessed with scales should identify the following:

- Accesses, exits, gates, approaches, and areas of anchorages, maneuvering and berthing;
- Cargo warehouse, storage spaces, terminals, and cargo handling equipment;
- Systems such as electricity supplies, Power plants, distribution, substations, radio, and telecommunication systems;
- Computer systems and networks;
- PF or ship traffic-management systems and to navigational aids;
- Cargo transfer piping, and fresh water supplies and all piping systems;
- Railways and roads Bridges;
- PF service supply boats, including pilot boats, tugs, lighters, etc.;
- Security and surveillance equipment, devices and systems;
- Waters adjacent to the PF.

– A detailed description of the current state of security in the PF including the accomplished performance review list.

– A detailed description of the nature of the PF being assessed.

– A prioritized listing of potential risks to be addressed.

It shall be advised that the PF operators have to ensure that the original security assessment is revised to take into account any changes concerning its operations, as well as changes in the PF structures or in the vicinities around the port facilities. A copy of this statement shall be enclosed in each PFSA report.

3.4.2. Security operations and security training records

The following additional records shall be maintained as the following:

- Training records: For every security training session, the date of every session, duration of the session, a description of the training and a list of attendees' names.
- Drills and exercises records: For every security drill or exercise, the date held, description of drill or exercise, list of participants' names and any best practices or lessons learned that could improve the PFSP.
- Security incidents and breaches records: For each security incident or breach, the date and time of occurrence, location in the PF, description of incident or breaches, to whom it was reported, and a description of the response.
- Changes in security levels records: For each change in security level, the date and time of notification received and time of compliance with additional requirements.
- Records of maintenance, calibration and testing of security equipment: For each occurrence of maintenance, calibrations and testing, the date and time and the specific security equipment involved.
- Records of security threats: For each security threat, the date and time of occurrence, how the threat was happened, who received or identified the threat, description of such threat, to whom it was reported and a description of the response.
- Records of Declaration of Security (DoS): A copy of every DoS for at least 90 days after its starting date.
- Records of the annual PFSP audit: For each annual audit, a letter certified by the PFSO documented the date such accomplished audit.

3.4.3. Retention of records

All records concerning the PFSA and PFSP shall be maintained until a new security assessment or security plan is accomplished. Unless otherwise specified in this document, all other records required in ISO 20858 shall be maintained for at least 2 years. Records could be kept in an electronic format. If so, they shall be secured against unauthorized disclosure, deletion, destruction or amendment.

4. The Proposed tiers of using ISO 20858 by port facilities

ISO 20858 directly concerns PFSAs& PFSPs development. It is designed to facilitate a consistent implementation of the ISPS code worldwide such a way creating a safe and secure

international maritime shipping system. In addition, it is designed to ensure that the completed work meets the requirements of IMO and the appropriate maritime security practices that can be verified by an outside auditor. It is a unique standard when compared with other ISO standards as it focuses only on the marine PF. This standard addresses the execution of marine PFSAs, marine PFSPs as well as the skills and knowledge necessary for the personnel involved in implementation of the ISPS Code (Teck& Shah, 2008).

The vital importance of PFs makes them a vulnerable node as a port-related disruption can generate domino effect on a network of supply chains (Loh&Thai,2014). The port facilities' failure to show an evidence of complying to ISPS code and other international necessary requirements could resulted in losing their commercial confidence among the shipping companies, ships operators, charterers, freight forwarders and other international industry players involving in maritime trade. Such failure could finally lead to lose the ports' competitiveness. It is the responsibility of port facilities to maintain their continuous compliance to the necessary international requirements and also port facilities had better display an evidence for the effectiveness of security procedures and measures implemented through a proved port facility security plan.

This Paper suggests that using ISO 20858: 2007 is a clear evidence for those port facilities executing an approved PFSP and emphasizing their compliance with the ISPS code as well as the other international necessary requirements. Accordingly, the Ships' masters and operators, shipping companies, charterers and freight forwarders will be sure that port facilities voluntary determine to use ISO 20858 fully meet the international mandatory industry-determined level of compliance with all needed requirements.

The critical importance of port facilities in the international trade operations makes them a vulnerable link in the supply chains because a disruption in port facilities' activities could generate a domino effect on the network of supply chains causing a profound negative effect on the entire global economy. The vulnerability of port facilities needs to ensure having an evidence of executing of an approved PFSP implementing all necessary international requirements to secure that vital link, port facilities, in the supply chains and as a result secure the global maritime trade. **Applying the three tiers in using ISO 20858 as:**

- The First Tier is a first party audit which is the self-verification of conformance by the port facility itself.
- The Second Tier is a second party audit which is the verification of a port facility's conformance to agreed criteria by another entity, agency or body which has a vested interest in the port facility's operations in the supply chain.
- The Third Tier is a third party audit which is the verification of conformance to agreed criteria by an entity independent of all parties of the port facility.
  Figure 2. indicates Three tiers using ISO 20858.

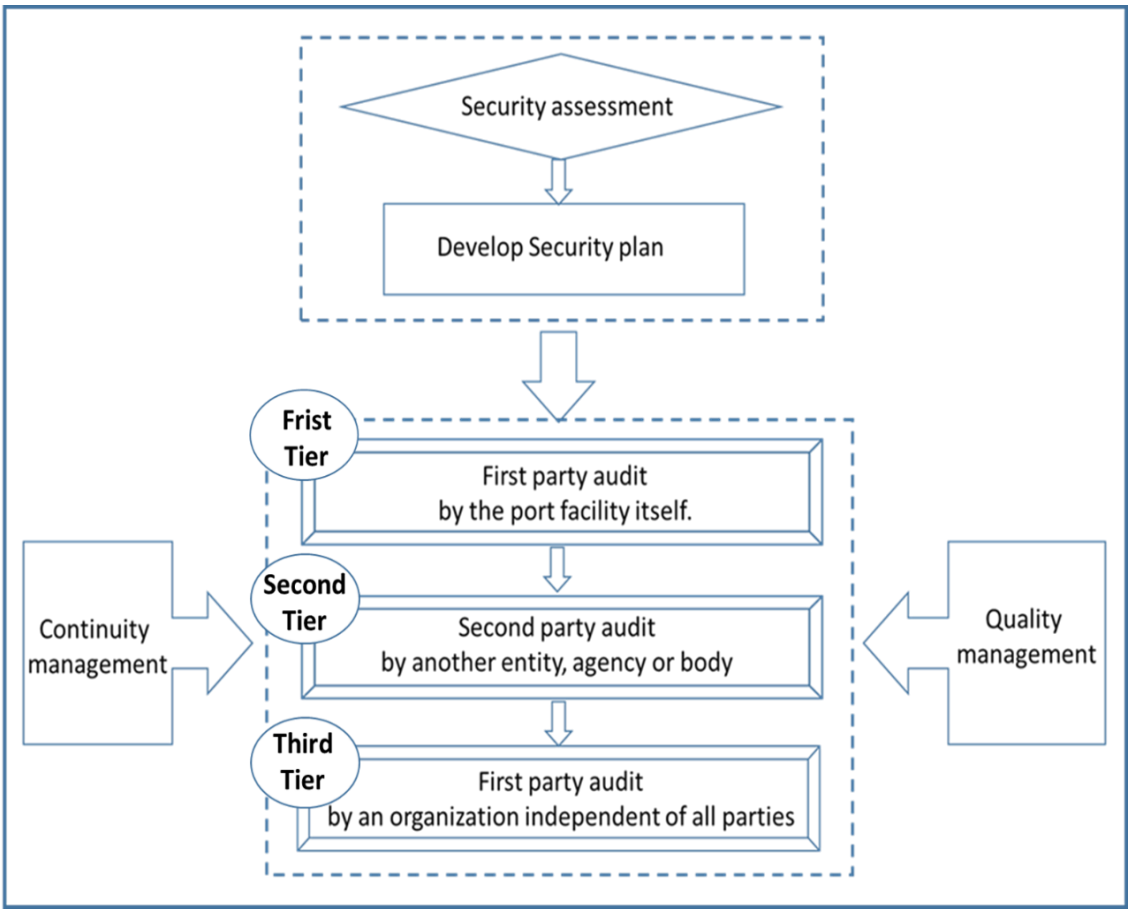

Figure 2. Three tiers using ISO 20858. Source: Prepared by authors

Port facilities that are intending to implement ISO 20858 are not obliged to obtain such services by an external consultant. In case of any port facility decides that it is necessary to have advice or consultant to conduct port facility security assessments, develop port facility security plans or implement the necessary requirements, it may seek external consulting services. However, it is the responsibility of the port facility seeking such consultant to completely verify the competence of consultants offering the advisory services.

Finally, consultants who offer such services to a port facility shall be excluded from participating in third party audits of the same port facility. Using ISO 20858 through the first and the second tier, a first party audit and a second part audit, will not cost any financial burdens on the port facilities. However, if having a document of compliance with ISO 20858 from a third party audit process is a target then the port facility seeking certification should consider selecting a third party certification body accredited by a competent accreditation body, such as a distinguished Recognized Security Organization (ISO,2007).

There are many port facilities using ISO 20858 as a clear and physical evidence to prove their compliance with the necessary requirement of the ISPS code. The first example, Arab Shipbuilding and Repair Yard (ASRY) has complied with ISO 20858 since 2010. ASRY has had

maritime business since 1977. Beginning with the dry-dock, followed by the floating docks, slipways, and over 4km of alongside berth space, ASRY now has a leading variety of facilities to repair any size and type of vessel. The yard is trusted by some of the most prestigious names in the global shipping industry and is capable of repairing any type and size of marine vessel, from workboats, to containerships, VLCCs, cargo vessels, ro-ro vessels, bulk and cargo carriers, chemical carriers, and more (ASRY, 2015). The second example, Dubai Port (DP) World has already conformed ISO 20858 - at its all terminals throughout the company's network of 77 operating marine and inland terminals supported by over 50 related businesses in 40 countries across six continents (DP World,2016,2017). Maritime Security Committee (MSC) 83 noted that ISO PAS 20858 was issued to uniform the implementation of the ISPS Code and It is considered as a full ISO standard (IMO,2008).

5.Conclusion and Recommendations

There is an urgent need for complying with the international maritime security standards. it is required an international support in dealing with necessary maritime security indicating that this is an international problem and national solutions or unilateral government actions would not work. There is an urgent need for complying with the international maritime security standards. it is required an international support in dealing with necessary maritime security indicating that this is considered as international problem. So, national solutions or unilateral government actions would not work effectively. ISO 20858 is a requirements standard intended to help port facilities executing an PFSPs to establish and demonstrate their compliance with the IMO regulations and ISPS code requirements in a manner that can be verified by an outside auditor.

Therefore, having a certificate of using ISO 20858 shall eliminate any doubt against the effectiveness and efficient of executing the port facility Security Plan. This research is to propose three tiers to use ISO 20858 and highlight the importance of having a certificate of ISO 20858 as a clear evidence of complying with the necessary international requirements through executing a proved PFSP. So, Ships' masters, operators and all maritime industry parties will be sure that such port facilities using ISO 20858 meet the international mandatory industry-determined level of compliance with the ISPS Code.

This paper recommends applying the three proposed tires of using ISO 20858:2007 in the Egyptian port facilities to have a clear evidence of their compliance to the international security requirements, increase their competitiveness, ensure preventing any attempt to breach the security of the port facilities.

References

1- Arab Shipbuilding & Repair Yard (ASRY), (2015), ASRY- Brochure, https://www.asry.net/wp -content/uploads/2015/08/ASRY-Brochure-Dec14-low-res.pdf (Accessed MAR 21, 2017).
2- CRISP (Evaluation and Certification Schemes for Security Products) project, (2014). Consolidated report on security standards, certification and accreditation – best practice and lessons learnt, http://crispproject.eu/ (Accessed MAR 26, 2017).

3- Chacon, H, Victor, (2016). “The Due Diligence in Maritime Transportation in the Technological Era”, PHD Dissertation, Faculty of Law, the University of Hamburg.
4- DP World Corporate Brochure, (2016). http://web.dpworld.com/wp-content/uploads/2014/01/DPW_Corporate-Brochure_A03.pdf (Accessed MAR 20, 2017).
5- DP World, (2017). ttp://dpworld.ae/uploads/Download/English/56962015114925PM845-DP%20World%20UAE%20Region%20Handbook%20English.pdf (Accessed MAR 11, 2017).
6- Hui, Shan, Loh. Vinh, Van, Thai, (2014). Managing Port-Related Supply Chain disruptions: A Conceptual Paper. The Asian Journal of Shipping and Logistics. Volume 30 (1) pp. (097-116).
7- International Organization for Standardization(ISO), (2007). ISO 20858:2007 Ships and marine technology – Maritime port facility security assessments and security plan development, Geneva.
8- International Labor Organization, (2004). ILO and IMO code of practice Security in ports. Geneva.
9- International Maritime Organization, (2008). MARITIME SAFETY COMMITTEE, 83th session, MSC 83/4, MEASURES TO ENHANCE MARITIME SECURITY, London.
10- Khalid, Bichou. Michael, G, H. Bell and Andrew, Evans, (2014). RISK MANAGEMENT IN PORT OPERATIONS, LOGISTICS AND SUPPLY-CHAIN SECURITY Routledge, New York, ,10017, USA.
11- Lee, Ghim, Teck. Muhammad, Zaly, Shah, (2008). SUPPLY CHAIN SECURITY FOR PORT FACILITY IN COMPLIANCE WITH ISPS CODE. EASTS International Symposium on Sustainable Transportation incorporating Malaysian Universities Transport Research Forum Conference 2008 (MUTRFC08).
12- Li, Yanqing, (2011). ISO/TC8 Bridge with IMO, http://www.asef2015.com/asef2007/PDF/1.%20ISO-IMO%20by%20Mr.Li%20(China)-1.pdf (Accessed Mar 19, 2017).
13- Mohamed, M, Abdel Fattah, (2015). PROPOSED INTEGRETED MODEL TO PORT FACILITY SECURITY MANAGEMENT AND PERFORMANCE MEASUREMENT. MASTER DEGREE Dissertation. Maritime Post graduate studies Institute. AASTMT. Egypt. Alexandria.
14- Periasamy, Gunasekaran, (2012). PORT SECURITY IN A DEVELOPING COUNTRY – PRE AND POST 9/11 TERRORIST ATTACKS: A CASE STUDY ON PORT KLANG IN MALAYSIA, PHD Thesis, Greenwich Maritime Institute, University of Greenwich, London.
15- ISO Focus ,(2006). Maritime security, The Magazine of International Organization for Standardization, Volume 3, Nos. 7/8, July/August 2006, ISSN 1729-8709, Genève, Switzerland.
16- UNCTAD, (2013). Review of Maritime Transport 2013., United Nation, Geneva.
17- UNCTAD, (2016). Review of Maritime Transport 2016., United Nation, Geneva.