DRAFT AMENDMENT ISO 28004:2007/DAmd 1

ISO/TC **8**

Secretariat: **SAC**

Voting begins on:
2010-09-01

Voting terminates on:
2011-02-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000

AMENDMENT 1: Medium and small ports

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Lignes directrices pour la mise en application de l'ISO 28000

AMENDEMENT 1: Ports petits et moyens

ICS 47.020.99

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

Amendment 1 to ISO :2010 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

Introduction

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote. Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. **ISO 28004**, "***Security Management Systems for the Supply Chain - Guidelines for the Implementation* of *ISO 28000*",** was prepared by Technical Committee **ISO/TC 8**, ***Ships and Marine Technology***, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain. This first edition of ISO 28004 cancels and replaces ISO/PAS 28004:2006, which has been technically revised. ISO 28000 is compatible with the ISO 9001:2000 (Quality) and ISO 14001:2004 (Environmental) management systems standards.

The "**ISO 28000:2007**, ***Specification for security management systems for the Supply Chain",*** and the guidance contained in ISO 28004, have been developed in response to the need for a recognizable supply chain management system evaluation criteria (validation process) against which their security management systems can be assessed and certified for determining conformance with the ISO 28000/28004 Standards. The guidance currently contained in ISO 28004 is designed to assist organizations adopting ISO 28000. Because the types of organizations that can use ISO 28000 are vast, the guidance provided in ISO 28004 is general in nature. As a result, some smaller organizations have had difficulty in defining the scope of measures needed to address each of the requirements established in ISO 28000. Therefore, the purpose of the Addendum is to provide guidance and amplifying information that can be used by Medium and Small seaports to assist them in defining the scope of validation and verification measures needed to comply with the security provisions specified in ISO 28000 and ISO 28004.

ISO 28000 requires that stakeholder organizations evaluate the capabilities of their security protection management plans and procedures through periodic reviews, testing, post-incident reports, and training exercises to measure the effectiveness of their installed security protection systems and methods. It is critical to the over all continued end-to-end safety of the supply chain that stakeholder organizations ensure to the transportation industry that they have sufficient safe guards in place to protect the integrity of the supply chain while those goods are under their direct control. The failure by one of the stakeholder organizations to protect the supply chain from any one of the global threats and operational risks can severally impact the integrity of the system and erode the confidence of those who depend on the secure transportation of their valuable goods.

The Medium and Small seaport stakeholder organizations are an integral part of the supply transportation system and will be required to conduct these performance capabilities reviews and verify to the transportation industry that they are in conformance with relevant legislation and regulations, industry best practices and conformance with its own security policy and objectives based on the identified threats and risks to their operations. The information contained in this Addendum provides for guidance and criteria for evaluating the quality of the seaport security management plans developed in accordance with ISO 28000 standards to protect the integrity of the supply chain. The amplifying information is designed to enhance, but not alter the general guidance currently specified in ISO 28004. No alterations to ISO 28004, other than the addition of supplements, will be undertaken.

Relationship with ISO Relevant Technical Standards

There are several established and pending related ISO technical standards that when coupled with this Addendum, provide additional guidance and instructions for the seaport operators for establishing their security management plans and evaluating the capability of those plans to protect the integrity of the supply chain cargo while under their direct control. These standards, ISO 20858, 28001, 28002, 28003, including 28004 are referenced in this Addendum and in order to provide specific guidance steps to Operators. The relevance of these standards to ISO 28000 is presented in the following Table.

ISO Technical Standard	**Technical Description**
ISO 28004	Provides guidance to certifying bodies on assessing conformance of an organization with the requirements of ISO 28000
ISO 20858	Provides a professional interpretation of the IMO ISPS for port facility security and guidance for evaluating the Port security management plans and installed operational procedures.
ISO 28001	Provides security requirements addresses the core security requirements of the World Customs Organization (WCO) Authorized Economic Operator Program
ISO 28002	Provides guidance on establishing a policy to enhance the resilience of an organization’s supply chain
ISO 28003	Provides guidance to certifying bodies on assessing conformance of an organization with the requirements of ISO 28000

Disclaimer

This International Standard does not purport to include all necessary provisions of a contract between supply chain operators, suppliers and stakeholders. Users are responsible for its correct application. Conformance with this International Standard does not of itself confer immunity from legal obligations.

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000

AMENDMENT 1: Medium and small ports

Page 56, add the following Annex B :

Annex B
(informative)

Guidelines for adopting ISO 28000 for use in medium and small seaport operations

1 Introduction/Overview

1.1 Objective

The objective of this Addendum to ISO 28004 is to provide guidance to medium and small ports that wish to adopt ISO 28000. This guidance provides a self-evaluation criterion that could be used by these ports as they implement ISO 28000. While the self certification criteria will not result in a 3rd party certification it can be used to determine the capability of the seaport stakeholders' security management plans for safeguarding the integrity of supply chain in accordance with the security provisions and guidelines specified in the ISO 28000/28004 standard. The goal is to develop a risk assessment evaluation rating scale metric that can be used to evaluate the capability of the port security management plans to provide uninterrupted security protection and continuous operations for the supply chain cargo being received, stored, and transferred by the seaport. The use of these self-evaluation criteria will enable the user to determine if the seaport has addressed each requirement of ISO 28000 in adequate detail.

1.2 Scope

This document will provide an addendum to ISO 28004 that will identify supply chain risk and threat scenarios, procedures for conducting risks/threat assessments, and evaluation criteria for measuring conformance and effectiveness of the documented security plans in accordance with ISO 28000/28004 implementation guidelines. An output of this effort will be a level of confidence rating systems based on the quality of the security management plans and procedures implemented by the seaport to safeguard the security and ensure continuity of operations of the supply chain cargo being processed by the seaport. The rating system will be used a means of identifying a measurable level of confidence (on a scale 1 to 5) that the seaport security operations are in conformance with ISO 28000 Standards for protecting the integrity of the Supply Chain.

1.3 Background/Understanding

The International Ship and Port Facility Security (ISPS) Code requires that each maritime port facility develop a comprehensive port facility security plan that includes the cargo under their direct control. The port security plan should address those applications, security systems and operations measures designed to protect the personnel, port facilities, ships at berth, cargo, and cargo transport units, including rail and ground within the port facility physical boundaries from the risks of a security incident (ISO 20858 provides clear guidance on meeting these requirements). The ISO 28000/28004 Standard has established guidelines for protecting the Global Supply Chain at a very high level, but does not provide enough specific detail that would allow a consistent level of implementation to cover all of the security provisions and applications for large, medium and smaller seaports that are integral parts of the global supply chain security infrastructure. To ensure long term and consistent security of the supply chain, there is a need for each of the stakeholders in this integrated global network to be measured and held accountable for contributing to the safety and uninterrupted delivery of goods.

The Medium and Small seaports are an integral part of the supply chain delivery infrastructure especially considering that these ports are typically the first entry points for a majority of the goods being shipped and distributed to local and international destinations. These smaller ports are the feeder ports for goods being shipped to the larger- mega ports for consolidating cargo for distribution to long haul shipment to other mega ports and global destinations. Therefore, it is critical that these Medium – Small sized seaports implement and maintain proven security provisions that can ensure the protection and continued safe passage of goods being shipped through their port facilities.

While ISO 28000/28004 provides general overviews of the expected requirements to secure the Supply Chain, there are limited instructions, measurable requirements and acceptance criteria that would allow an entity to create and implement a security management plan that would ensure that the established standards in ISO 28000 were met. Therefore, this Addendum is designed to provide the methods, procedures, guidelines and acceptance criteria that will be used for measuring the level of conformance with ISO28004 security provisions.

1.4 ISO 28000 Requirements for Security Risk Assessment (4.3.1)

In accordance with the ISPS Code requirement and the security risk assessment requirements specified in paragraph 4.3.1 of ISO 28000, the Seaport stakeholders and governing organization shall establish and maintain procedures for the ongoing identification and assessment of security threats, security management-related threats and risks, and the identification and implementation of the necessary management control measures to safeguard the supply chain. The Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the seaport operations. This assessment shall consider the likelihood of an event and all of its consequences to the seaport stakeholders, threats to continuity of operations, supply chain security, and disaster recovery. Specifically, the risk assessment should address at a minimum, the following:

a) Physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action.

b) Operational threats and risks, including the control of the security, human factors and other activities, which affect the organizations performance, condition or safety.

c) Natural environmental events (storms, floods, high winds, etc.), which may render security measures and equipment ineffective.

d) Factors outside of the organization’s control, such as failures in externally supplied equipment and services, changes in local and international security policies and regulations, and political changes affecting seaport ownership and operations.

e) Stakeholder threats and risks such as failure to meet regulatory requirements, financial constraints, or ownership changes that affect port operations and supply chain security.

f) Design, installation, validation and maintenance of security equipment including installation of new systems and training of staff to operate, repair and maintain.

g) Failure of critical Information, data management and communication systems used to manage and safeguard the supply chain.

The seaport stakeholder organizations responsible for providing security protection for supply chain goods shall ensure that the results of these assessments and the appropriate security controls are in place to safeguard the integrity of the supply chain. The seaport Security Management Plan must provide provisions and procedures for addressing the security system objectives, operational requirements, risk assessment and mitigation, continuity of operations and disaster recovery steps. Specifically, the plan should address the following:

a) The determination of requirements for the design, specification, installation, certification and operation of security devices and systems;

b) Identification of security staffing resources, skill levels, and training needed to operate and maintain security devices and systems (ISO 28000/4.4.2);

c) Identification of the organization's overall threat and risk assessment and management framework to mitigate identified risks.

d) Continuity of operation provisions and disaster recovery steps that will be implemented to restore security systems for protecting the supply chain and restore the seaport to full operational status.

The organization shall document and keep the above information up to date and have personnel trained in the understanding and application of the security and operational plans and procedures specified in the plan. The organization's methodology for threat and risk identification, assessment and mitigation shall at a minimum do the following:

a) Be clearly defined with respect to its scope, stakeholder roles and responsibilities, expected nature and timing of risks and threats to ensure it is proactive rather than reactive.

b) Identify and the monitor the collection of information sources to document existing and determine future supply chain related security threats and risks.

c) Provide for the classification of threats and risks and the identification of mitigation steps for those that must be either avoided, eliminated or controlled.

d) Provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation (ISO 28000/4.5.1) to ensure uninterrupted protection of the supply chain.

The should be a planned part of the continuous improvement procedures for keeping the seaport personnel and systems current with identified threats, risks and operational security needs required to safeguard the supply chain.

The security threat identification, risk assessment and risk management processes and their outputs should be the basis for developing and implementing a comprehensive supply chain security system. It is important that the links between the security threat identification, risk assessment and risk management processes and the other elements of the security management system are clearly established, continually monitored and updated to reflect any changes in the threats and risks assessments to port operations for safeguarding the supply chain.

1.5 Risk Assessment Requirements

1.5.1 General

Security threat identification, risk assessment and risk mitigation processes are key tools in the management, control and elimination of risks to the security and continuous operation of the supply chain. The seaport security management plan must address each of these areas and provide specific roles and responsibilities for each stakeholder involved in safeguarding the supply chain.