PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28001

First edition
2006-09-01

Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Meilleures pratiques pour la mise en application de la sûreté de la chaîne d'approvisionnement — Évaluations et plans

Reference number
ISO/PAS 28001:2006(E)

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.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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/PAS 28001 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 11, *Intermodal and short sea shipping*.

Introduction

Security incidents against international supply chains are threats to international trade and the economic growth of trading nations. People, goods, infrastructure and equipment, including means of transport, should be protected against security incidents and their potentially devastating effects. Such protection benefits the economy and society as a whole.

International supply chains are highly dynamic and consist of many entities and business partners. This Publicly Available Specification recognizes this complexity. It has been developed to allow an individual organization in the supply chain to apply its requirements in conformance with the organization's particular business model and its role and function in the international supply chain.

This Publicly Available Specification is an option for organizations to establish and document reasonable levels of security within international supply chains and their components. It will enable such organizations to make better risk based decisions concerning the security in those international supply chains.

This Publicly Available Specification is multimodal and is intended to be in concert with and to complement the World Customs Organization's Framework of Standards to secure and facilitate global trade (Framework). It does not attempt to cover, replace or supersede individual customs agencies' supply chain security programmes and their certification and validation requirements.

This Publicly Available Specification is a voluntary specification to help organizations to establish adequate levels of security within those part(s) of an international supply chain which they control. It is also a basis for determining or validating the level of existing security within such organizations' supply chain(s) by internal or external auditors or by those government agencies that choose to use compliance with this Publicly Available Specification as the baseline for acceptance into their supply chain security programmes. Customers, business partners, government agencies and others may request organizations which claim compliance with this Publicly Available Specification to undergo an audit or a validation to confirm such compliance. Government agencies may find it mutually agreeable to accept validations conducted by other governments' agencies. If a third party organization audit is to be conducted, then the organization should consider employing a third party certification body accredited by a competent body, which is a member of the International Accreditation Forum (see Annex C).

It is not the intention of this Publicly Available Specification to duplicate governmental requirements and standards regarding supply chain security in compliance with the WCO Framework. Organizations that have already been certified or validated by mutually recognizing governments are compliant with this Publicly Available Specification.

Outputs resulting from this document will be the following.

- A Statement of Coverage that defines the boundaries of the supply chain that is covered by the security plan.

- A Security Assessment that documents the vulnerabilities of the supply chain to defined security scenarios. It also describes the impacts expected from each of the potential threat scenarios.

- A Security Plan that describes security measures in place to manage the security threats identified by the Security assessment.

- A training programme setting out how security personnel will be trained to meet their assigned security related duties.

To undertake the security assessment needed to produce the security plan, an organization using this Publicly Available Specification will

- identify the threats posed (security scenarios);
- determine how likely persons could carry out each of the security scenarios identified by the Security Assessment.

This determination is made by reviewing the current state of security in the supply chain and, based on the findings of that review, professional judgment is used to identify how vulnerable the supply chain is to each security scenario.

If the supply chain is considered unacceptably vulnerable to a security scenario, the organization will develop additional procedures or operational changes to lower likelihood, consequence or both. These are called countermeasures. Based upon a system of priorities, countermeasures should be incorporated into the security plan to reduce the threat to an acceptable level.

Annexes A and B are illustrative examples of risk management based security processes for protecting people, assets and international supply chain missions. They facilitate both a macro approach for complex supply chains and/or more discrete approaches for portions thereof.

These annexes are also intended to

- facilitate understanding, adoption, and implementation of methodologies, which can be customized by organizations;
- provide guidance for baseline security risk management for continual improvement;
- assist organizations to manage resources to address existing and emerging security risks;
- describe possible means for assessment of risk and mitigation of security threats in the supply chain from raw materiel allocation through storage, manufacturing, and transportation of finished goods to the market place.

Annex C provides guidance for obtaining advice and certification for ISO/PAS 28001 if an organization using this Publicly Available Specification chooses to exercise this option.

Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans

1 Scope

This Publicly Available Specification provides requirements and guidance for organizations in international supply chains to

- develop and implement supply chain security processes;
- establish and document a minimum level of security within a supply chain(s) or segment of a supply chain;
- assist in meeting the applicable Authorized Economic Operators criteria set forth in the World Customs Organization Framework of Standards and conforming national supply chain security programmes.

NOTE Only a participating National Customs Agency can designate organizations as Authorized Economic Operators in accordance with its supply chain security programme and its attendant certification and validation requirements.

In addition, this Publicly Available Specification establishes certain documentation requirements that would permit verification.

Users of this Publicly Available Specification will

- define the portion of an international supply chain they have established security within (see 4.1);
- conduct security vulnerability assessments on that portion of the supply chain and develop adequate countermeasures;
- develop and implement a supply chain security plan;
- train security personnel in their security related duties.

2 Normative references

The following referenced documents may be required for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/PAS 20858, *Ships and marine technology — Maritime port facility security assessments and security plan development*

International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, International Maritime Organization