CTN Newsletter Special Bulletin
Enhancing Container and Supply Chain Security
July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", *OSCE Ministerial Council Decision No.9/04*

Supply Chain Security Management Update ISO 28000 Series

CAPT Charles H. Piersall, Chairman, Technical Committee on Ships and Marine Technology (TC8)
International Standardization Organization (ISO)

Coast Guards patrolling the harbour area of the port of Batumi, Georgia, May 2010 (OSCE/Mehdi Knani)

INTRODUCTION

This article will provide some background, examples of implementation and the current status of the ISO 28000 family of standards.

There are many new "buzzwords" being introduced into the topic of "security and security management and the safety and security of the supply chain" and some are coming from sources with no practical experience or understanding of what is needed by participating decision makers in the supply chain. First, let's clarify the "supply chain". It is not a simple, single linking of elements in a chain. It is a complex network of many links and nodes which is tailored to meet the needs of the particular organization, industry and government regulatory requirements. Along with many of these "buzzwords" are often attempts to create additional layering of management systems standards, redefining the security regime and imposing additional certification requirements. This approach not only adds confusion, but additional unwarranted costs to the industry.

ISO 28000 serves as the "umbrella" management system standard which reduces financial burden while enhancing overall security performance by successfully planning for and successfully recovering from any disruptive event. It establishes a management system framework that can be used to cover all aspects of security- assessing risk, emergency preparedness, business continuity, sustainability, recovery, resilience and/or disaster management - relating to terrorism, piracy, cargo theft, fraud, and many other security disruptions. Organizations may tailor an approach compatible with their existing operating systems. Those who have adopted a process approach to management systems may be able to use their existing system as a foundation for a security management system as prescribed in ISO 28000.

ISO 28000 is the only published and certifiable International Standard that takes a holistic, **risk-based approach to managing risks associated with any disruptive incident in the supply chain -before, during and after the event. It suggests how to improve resilience and preparedness performance in a cost effective way based on a plan-do-check-act (PDCA) management system modeled after the proven framework and risk-based approach outlined in ISO 14001. PDCA** can be described as follows.

- Plan: establish the objectives and processes necessary to deliver results in accordance with the risk assessment
- Do: implement the processes.
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- Act: take actions to continually improve performance of the security management system.

ISO 28000 (Section 4.3.1) states, in part, **"risk assessment** shall consider the likelihood of an event and all of its consequences which shall include: **physical failure threats and risks**, such as functional failure, incidental damage, malicious damage or terrorist or criminal action; **operational threats and risks,** including the control of the security, human factors and other activities which affect the organizations performance, condition or safety; **natural environmental events** (storm, floods, etc.), which may render security measures and equipment ineffective; **factors outside of the organization's control**, such as failures in externally supplied equipment and services; and **stakeholder threats and risks** such as failure to meet regulatory requirements or damage to reputation or brand;…."

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", *OSCE Ministerial Council Decision No.9/04*

ISO 28000 security plan strategy is to better prepare for disruptions and proactively manage risks through cost effective measures.

ISO 28000 (Section 4.4.7) on **Emergency preparedness, response and security recovery** states "The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them.

BACKGROUND

The following are quotes from ISO Press Release on publication of ISO 28000:

"ISO: Geneva - **Reducing Piracy, Fraud, and Terrorism** - The ISO 28000 series of standards on supply-chain security-management systems will help to reduce risks to people and cargo. The standards address potential security issues at all stages of the supply process, thus **targeting threats such as piracy, fraud, and terrorism.**

ISO Secretary-General stated: "**Threats in the international market-place know no borders," The ISO 28000 series provides a global solution to this global problem. With an internationally recognized security-management system, stakeholders in the supply chain can ensure the safety of cargo and people, while facilitating international trade, thus contributing to the welfare of society as a whole."**

The ISO 28000 series of international standards can be applied by organizations of all sizes involved in manufacturing, service, storage, or transportation by air, rail, road, and sea at any stage of the production or supply process.

The ISO 28000 series will facilitate trade and the transport of goods across borders. It will increase the ability of organizations in the supply chain to effectively implement mechanisms that address security vulnerabilities at strategic and operational levels, as well as to establish preventive action plans. Organizations can then continually assess their security measures to protect their business interests, and ensure compliance with international regulatory requirements. By encouraging the implementation of these standards by the various actors in the supply chains, countries will be able to maximize the use of government's resources, while maintaining a level of optimal security.

The ISO 28000 series assists in implementing governmental and international customs-agency security initiatives, including the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade, the EU Authorized Economic Operators Programme, the U.S. Customs Trade Partnership against Terrorism, and the International Maritime Organization's (IMO) International Ship and Port Facility Security Code." *End of quote*

Container ship docked at the port of Poti, Georgia, May 2010 (OSCE/Mehdi Knani)

The ISO 28000 series specifies the requirements for a security management system to ensure security in the supply chain network... **The standards address potential security issues at all stages of the supply process from point of manufacture, including sources of financing, to the final consumer thus targeting threats such as terrorism, fraud and piracy**. It involves many entities such as producers of the goods, logistics management firms, consolidators, truckers, railroads, air carriers, marine terminal operators, ocean carriers, passenger ships, ferries and inland transport, cargo/mode/customs agents, financial and information services, and buyers of the goods being shipped for all links in the supply chain.

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", *OSCE Ministerial Council Decision No.9/04*

The security problem is one that is shared by government and industry, and meaningful solutions must reflect that global partnership. It is a problem shared by companies, large and small, involved in the secure transport of goods and movement of people.

(OSCE/Mehdi Knani)

IMPLEMENTATION

The ISO 28000 series is being implemented and certified in a variety of industries worldwide. Some examples of widely diverse industries are:

- **DP World** was **first to certify a marine terminal** and will complete ISO 28000 certifications throughout its network of 48 terminals in 31 countries worldwide by 2012. DP World is the only global marine terminal operator to have achieved simultaneous ISO 28000 certification and C-TPAT membership. Its European terminals were certified as Approved Economic Operator (AEO) by the European Union.
- **Port of Houston Authority,** one of the world's largest ports, was the **first port authority in the world to attain ISO 28000 certification**.
- **YCH Group,** Singapore, is the **first supply chain management (SCM) company to be ISO 28000 certified.** YCH Group is the leading integrated end-to-end supply chain management and logistics partner to some of the world's largest companies including Canon, Dell, Moet-Hennessy, ExxonMobil, B. Braun, LVMH, Royal Friesland Campina and Motorola.
- **TNT Express' Asia regional head office in Singapore** is the **first express integrator to achieve certification to ISO 28000.**
- **YCH India is** also **certified** TAPA 'A-class' and ISO **28000-compliant** for its security systems. YCH India provides customized Supply Chain solutions for Electronics, Consumer Goods, Chemicals/Healthcare and Automotive industries in India. Its clientele includes DELL, ACER, TPV, General Mills, HCL and others.
- **DB Schenker**, the world's **second-largest forwarder**, obtained **ISO 28000 certification for its regional head office for the Asia-Pacific sector** in Singapore last year, along with its local office and operations at Singapore Changi airport. Klaus Eberlin, chief operating officer for the Asia-Pacific, views the **ISO standard as a "kind of umbrella standard that encompasses elements like the TAPA programs. ISO 28000 extends beyond physical aspects of security to elements like information flow and financial data".**

Other ISO 28000-certified companies include: **Asian Terminals** (first marine terminal in Philippines), **CTS Logistics**-China (kitting assembly of turnkey management of consumer electronic, IT and telecommunication products), **Banner Plasticard** - Philippines (design and printing of cards, personalization, embossing, encoding, thermal printing, wrapping crating and palletizing). There are also airport, railroad, pharmaceutical, health care, and high tech industries certifying to ISO 28000, and many other global industries.

Professional training for security and non practitioners using ISO 28000 is being conducted for (1) supply chain business operators and (2) Customs Officers.

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", *OSCE Ministerial Council Decision No.9/04*

ISO 28000 SERIES SATUS

- **ISO 28000:** Supply chain security management systems – **Published**: the overall "umbrella", certifiable, management systems standard.
- **ISO 28001:** Best practices for implementing supply chain security, assessments and plans – **Published:** designed to assist industry meet requirements for Authorized Economic Operator (AEO).
- **ISO 28002,** Resilience in the Supply Chain – Requirements with guidance for use – **PAS in publication:** This standard is to provide additional focus on resilience. It supports the strong demand as firms are looking for assurance that their suppliers and the extended supply chain have planned for steps to prevent and mitigate the threats and hazards to which they are exposed. As part of the ISO 28000 management system, the ISO 28002 standard emphasizes the need for an on-going, interactive process to prevent, respond to and assure continuation of an organization's core operations after a major disruptive event.
- **ISO 28003**, Auditing & Certification – **Published**: guidance for accreditation & certification bodies.
- **ISO 28004**, Guide for implementing ISO 28000 – **Published**: assist users in implementation.
- **ISO 28004**, **Addenda:** Additional guidance for adopting & certifying ISO 28000:

  Amd1 – for use in medium & small seaport operations – **Draft for voting**

  Amd2 – adopting ISO 28000 for small-medium sized businesses (SME) This specific guidance supplement will help medium and small businesses develop processes that comply with the general guidance contained in existing ISO 28004.

  Amd3 – for security requirements for Authorized Economic Operator – to provide specific guidance to organizations seeking to incorporate requirements contained in ISO 28001 for Authorized Economic Operators into their implementation of ISO 28000. The security best practices contained in ISO 28001 were carefully developed in liaison with WCO – **PAS approved to publish.**

- **ISO 28005**, Computer applications – Electronic port clearance (EPC) is the latest addition to the series. It provides for computer-to-computer data transmission. The details of this standard development have been briefed to IMO and WCO. To expedite the development, ISO 28005 has been broken into two parts:

  ISO 28005-1: Single window implementation – **Approved Work Item.** Republic of Korea (KATS) as new Project Leader

  ISO 28005-2: Core data elements – **PAS Published; DIS approved 2010-05-14**. Norway (MARINTEK e-Maritime) as Project Leader

Malta's transshipment port, Freeport, December 2009 (OSCE/Mehdi Knani)

- **ISO 28006**, Security management of RO-RO passenger ferries – **Under development**: best practices for application of security measures
- **ISO 20858**, Uniform implementation of ISPS Code – **Published**

NOTE

CAPT. Charles H. Piersall has been Chairman of ISO/TC8 since 1995. His committee is a recipient of the Lawrence D. Eicher Leadership Award. A retired United States Navy Captain, he has over 54 years of distinguished maritime service – first as a senior naval officer and then as a senior industry executive. In addition to the highest military awards, he is also recipient of numerous high level awards based on his contributions to international standardization.