MEASURES TO ENHANCE MARITIME SECURITY

ISO Maritime and supply chain security standards (Update)

Submitted by ISO

<table>
<thead>
<tr>
<th>SUMMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Executive summary:</strong></td>
</tr>
<tr>
<td><strong>Strategic direction:</strong></td>
</tr>
<tr>
<td><strong>High-level action:</strong></td>
</tr>
<tr>
<td><strong>Planned output:</strong></td>
</tr>
<tr>
<td><strong>Action to be taken:</strong></td>
</tr>
<tr>
<td><strong>Related documents:</strong></td>
</tr>
</tbody>
</table>

Introduction

1 The ISO 28000 series of international standards on supply chain security management systems, which have been upgraded from their status of Publicly Available Specifications to that of fully fledged International Standards, will help to reduce risks to people and cargo within the supply chain. 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.

2 This includes the movement of the goods, the shipping data, and the associated processes as well as the series of dynamic relationships. 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 nodes in the supply chain. The transport 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.
3 The ISO 28000 series of international standards specifies the requirements for a security management system to ensure security in the supply chain. Its standards can be applied by organizations of all sizes involved in manufacturing, service, storage or transportation by all modes of transport at any stage of the production or supply process. The series includes provisions to:

- establish, implement, maintain and improve a security management system;
- assure conformity with security management policy;
- demonstrate such conformity;
- seek certification/registration of conformity by an accredited third party organization; or
- make a self-determination and self-declaration of conformity.

4 MSC 83 noted that “the ISO 28000 series of standards on supply chain security were now published and numerous ports, terminals and organizations were being certified by third party independent accredited auditors; the ISO PAS 20858 for uniform implementation of the ISPS Code was now being published as a full ISO standard; and ISO standards could be applied to all ships, irrespective of size, type, purpose and whether operated internationally, domestically or within internal waters”.

Status of ISO supply chain initiatives

5 ISO has now published five maritime and supply chain standards replacing the originally published Publicly Available Specifications documents. Courtesy copies of the five standards have been provided to the Secretariat to assist the Committee. ISO 28000, ISO 28001, ISO 28003, ISO 28004 and ISO 20858 are also available from ISO national member institutes and from the ISO Central Secretariat. The standards are:

.1 ISO 20858:2007 on Ships and marine technology – Maritime port facility security assessments and security plan development, was published on 2007-10-15. It replaces the PAS which had been previously published 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;

.2 ISO 28000:2007 on Specification for security management systems for the supply chain, outlines the requirements to enable an organization to establish, implement, maintain and improve a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations.

While ISO 28000:2007 can be implemented on its own, it is designed to be fully compatible with ISO 9001:2000 and ISO 14001:2004 and companies already using these management system standards may be able to use them as a foundation for developing the security management system of ISO 28000. To help users to do so, ISO 28000 includes a table showing the correspondence of its requirements with those of ISO 9001:2000 and ISO 14001:2004;
ISO 28001:2007 on Security management systems for the supply chain – Best practices for implementing supply chain security – Assessments and plans – Requirements and guidance, will assist industry to meet best practices as outlined in the SAFE Framework of Standards to Secure and Facilitate Global Trade adopted by the World Customs Organization (WCO), the EU Customs Security Program-Authorized Economic Operator (AEO), and the US Customs and Border Protection initiative – Customs Trade Partnership against Terrorism (CTPAT);

ISO 28003:2007 on Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems, references ISO 19011:2002 on Guidelines for quality and/or environmental management systems auditing and ISO/IEC 17021 on Conformity assessment – Requirements for bodies providing audit and certification of management systems with any necessary security related modifications or change; and


ISO 28005 on Ships and marine technology – Computer applications – Electronic port clearance (EPC) is currently being developed and is the latest addition to the series. It provides for computer-to-computer data transmission. Referenced material includes European MarNIS project, EDIFACT standard developed by UNECE, UN/EDIFACT, IMO FAL forms, ports using XML technology, SafeSeaNet (EC directive) and Inland Waterways (UNECE WG on information technology). The details of this standard development have been briefed to the Maritime Security Working Group previously.

Certification of ISO 28000

ISO 28000 is being certified worldwide by third part independent auditors. A number of ports and terminals are in various stages of being certified. The Committee will be advised of progress periodically. The listing below shows current results:

DP World was the first company in the world to certify to the ISO 28000, certifying their corporate offices in Dubai, United Arab Emirates, and their terminal in Djibouti in September 2006;

Subsequently, the first marine terminal in the Americas was DP World Vancouver, Canada which was certified on 4 March 2007 and the Latin American gateway to the USA at Puerto Caucedo, Dominican Republic, which was certified on 9 April 2007;

Terminals at Southampton and Tilbury, United Kingdom; Antwerp Gateway and Antwerp Delwaidedock, Belgium; and Jebel Ali, United Arab Emirates, have all been certified, with Jebel Ali as the most recent one on 17 December 2007; and

DP World in its press release of 17 December 2007 stated that “DP World’s adoption and global implementation of the ISO standard means that its network of terminals will have the ability to effectively implement mechanisms and processes to address security vulnerabilities at strategic and operational levels. All terminals will be required to continually assess security measurements in place to both protect its business interests and ensure compliance with international regulatory...
requirements. The standard complements all international security legislative codes DP World already conforms to at its terminals. The independently audited standard (ISO 28000) is currently being rolled out throughout the company’s network of 42 terminals”. DP World operates, in 28 countries, 42 terminals, has 13 new developments and its activities span five continents.

Other related ISO 28000 and ISO 20858 matters

8 The Committee decided to develop non-mandatory guidance for the enhancement of security of non-SOLAS vessels. The ISO 28000 series, which are voluntary industry standards, are applicable to all vessels, all sizes, all types, in all trades, international, domestic and inland waters. Accordingly ISO, as a NGO, offers its assistance to participate in the Correspondence Group established by the Committee for the development of the aforesaid guidance where it may be beneficial to the group.

9 ISO, as a result of informal discussions, has concluded that some additional guidance for “smaller ports” in implementation of the ISO security standards may be useful. While it is true that the ISO standards are applicable to all organizations, large and small, it may be of benefit to provide additional guidance information to be of assistance to smaller ports with less resources. ISO is investigating what may be of value and will inform the Committee as the related work is progressed.

Action requested of the Committee

10 The Committee is invited to note the information provided, and take action as deemed appropriate.