ECONOMIC COMMISSION FOR EUROPE

INLAND TRANSPORT COMMITTEE

Multidisciplinary Group of Experts on Inland Transport Security

Second session
Geneva, 9-10 October 2007
Item 4 of the provisional agenda

Informal document AC.11 No. 11 (2007)

4 October 2007

ENGLISH ONLY

REGULATORY INITIATIVES AT THE INTERNATIONAL LEVEL

Submitted by the United Nations Conference on Trade and Development (UNCTAD)

WORK OF UNCTAD IN THE FIELD OF MARITIME TRANSPORT SECURITY

In the context of its continuing mandate in the field of transport and trade facilitation, as set out in the Sao Paulo Consensus,[1] UNCTAD has been monitoring current and emerging international developments on transport security, particularly developments at the IMO, the WCO and the EU, as well as in individual countries, and has analyzed some of the possible implications of such measures for developing countries. UNCTAD has issued a number of reports and other relevant publications in this respect, in particular the following:

UNCTAD Reports

- **CONTAINER SECURITY: Major Initiatives and Related International Developments, (UNCTAD/SDTE/TLB/2004/1)**

This report provided an overview over measures, initiatives and international developments relevant to maritime container security and offered some preliminary analysis of their potential impacts for the trade and transport of developing countries.
The full text of the report is available from the UNCTAD website: www.unctad.org/ttl/legal.

- **Maritime Security: ISPS Code Implementation, Costs and Related Financing (UNCTAD/SDTE/TLB/2007/1)**

In 2002, a new international maritime security regime was adopted, under the auspices of the IMO as part of the 1974 Safety of Life at Sea Convention (SOLAS). The International Ship and Port Facility Security Code (ISPS Code) imposes wide-ranging obligations on governments, shipping companies, and port facilities which were required to be implemented by 1 July 2004. In order to

[1] See Sao Paulo Consensus, TD/410, paragraphs 59 and 41.

help assess the costs associated with the ISPS Code, as well as their potential economic implications, UNCTAD conducted a global study based on a set of questionnaires designed to obtain first hand information from all affected parties. The main objective was to establish the range and order of magnitude of the ISPS Code-related expenditures made from 2003 through 2005 and to gain insight into the financing mechanisms adopted or envisaged. In addition the study sought to clarify matters relating to the implementation process, level of compliance and other less easily quantifiable impacts. The full text of the report, reflecting the results of the survey, is available from the UNCTAD website: www.unctad.org/ttl/legal.

UNCTAD Review of Maritime Transport

In addition to substantive reports, UNCTAD has published some information on international maritime and supply-chain security developments in its annual "**Review of Maritime Transport**". The 2007 issue is expected to be published soon. Copies of the review of Maritime Transport are available to download from the UNCTAD website at: www.unctad.org/ttl. Below are relevant extracts from the 2005 and 2006 issues.

Other UNCTAD Publications

Information on security-related developments is also provided in UNCTAD's quarterly "Transport Newsletter". Full text of the newsletter is available from the UNCTAD website: www.unctad.org/ttl. For some recent security articles see the following issues: No.34, Fourth Quarter 2006, and No.35, First Quarter 2007.

Excerpts from Relevant Issues of the Review of Maritime Transport

***Review of Maritime Transport, 2005*:**
"Developments in International Maritime Security: Entry into Force of the ISPS Code

Internationally, one of the most important recent developments in the field of maritime security was the entry into force, on 1 July 2004, of the International Ship and Port Facility Security Code (ISPS Code).[2] In December 2002, the International Maritime Organization (IMO) had adopted the ISPS Code as part of an additional chapter[3] to the 1974 Safety of Life at Sea Convention (SOLAS). The Code, together with a number of other amendments to SOLAS,[4] provides a new comprehensive security regime for international shipping.[5] It applies to all cargo ships of 500 gross tonnage or above, passenger vessels, mobile offshore drilling units and port facilities serving such ships engaged in international voyages.[6] Part (A) of the Code establishes a list of mandatory requirements, and Part (B) provides recommendations on how to fulfill each of the requirements set out in Part (A).
The new security regime imposes a wide range of responsibilities on governments, port facilities and ship-owning and -operating companies. These responsibilities were described in some detail and with appropriate references to the respective provisions of the Code in an earlier UNCTAD report.[7] However, for ease of reference, the main obligations are briefly summarized here.

Responsibilities of Contracting Governments

The principal responsibility of Contracting States under SOLAS chapter XI-2 and Part (A) of the Code is to determine and set security levels. Responsibilities also include, *inter alia*:

- approval of *Ship Security Plans*
- issuance of *International Ship Security Certificates* (ISSC) after *verification*
- carrying out and approval of *Port Facility Security Assessments*
- approval of *Port Facility Security Plans*
- *determination of port facilities* which need to designate a *Port Facility Security Officer*
- exercise of *control and compliance measures*.

Governments may delegate certain responsibilities to Recognized Security Organizations (RSO) outside Government.

---

[2] For the complete text of the ISPS Code, see SOLAS/CONF.5/34, Annex 1. See also *The International Ship and Port Facility Security Code*, 2003 Edition, ISBN 92-801-5149-5. For further information, see the IMO website (www.imo.org). Please note that all ISPS-related circulars issued by the IMO are available on the website under "legal", "maritime security".

[3] Chapter XI-2 on "Special measures to enhance maritime security".

[4] Chapters V and XI of the annex to SOLAS were amended, the latter chapter being renumbered as chapter XI-1.

[5] Cf. ISPS Code (A), Art. 1.2.

[6] See SOLAS, chapter XI-2/2 and ISPS Code (A), Art. 3.

[7] *Container Security: Major Initiatives and Related International Developments,* UNCTAD/SDTE/TLB/2004/1, paras. 80–86 (www.unctad.org).

Responsibilities of vessel-owning and/or -operating companies

Vessel-owning and/or -operating companies have a number of responsibilities, chief among which is to ensure that each vessel a company operates obtains an *International Ship Security Certificate* (ISSC) from the administration of a flag state or an appropriate RSO, such as a classification society. In order to obtain an ISSC, the following measures must be taken:

- designation of a *Company Security Officer* (CSO)
- carrying out *Ship Security Assessments* (SSA) and development of *Ship Security Plans* (SSP)
- designation of a *Ship Security Officer* (SSO)
- training, drills and exercises

A number of special mandatory requirements in SOLAS chapters V, X-1 and X-2 apply to ships and create additional responsibilities for vessel-owning companies and for Governments. These include in particular the following:

- *Automatic Identification System* (AIS)
- *Ship Identification Number* (SIN)
- *Ship Security Alert System* (SSAS)
- *Continuous Synopsis Record* (CSR)

Responsibilities of port facilities

Depending on size, there may be, within the legal and administrative limits of any individual port, several or even a considerable number of port facilities for the purposes of the ISPS Code.

- *Port Facility Security Plans* (PFSP): based on the *Port Facility Security Assessment* carried out and, upon completion, approved by the relevant national Government, a *Port Facility Security Plan* needs to be developed.
- *Port Facility Security Officer* (PFSO): For each port facility, a Security Officer must be designated.
- Training drills and exercises

Both Governments and industry faced the challenging task of implementing the various new security requirements within a short timeframe, by 1 July 2004. Full and complete compliance by that date was crucial, as the repercussions of non-compliance could be severe.[8] Efforts to ensure compliance intensified in the weeks and days prior to the deadline date, and continued in the period immediately afterwards. Despite the initially slow progress in implementation of the ISPS Code, figures provided by IMO member Governments indicate that by 1 July 2004, more than 86 per cent of ships and 69 per cent of declared port facilities had security plans approved.[9] By August 2004, the IMO reported that 89.5 per cent of over 9,000 declared port facilities had had their Port Facility Security Plans approved and "well beyond 90 per cent" of all ships had been issued International Ship Security Certificates, which indicated that almost complete compliance with the new IMO security measures was being achieved. However, according to the IMO, the picture was uneven, with "regional pockets in which progress had not been as rapid as might be hoped". Africa and the

[8] For further details on control and compliance measures, see UNCTAD report *Container Security: Major Initiatives and Related International Developments,* UNCTAD/SDTE/TLB/2004/1, para. 85 (www.unctad.org).

[9] See Press Briefing of 1 July 2004, *Secretary-General Mitropoulos pays tribute to the efforts made to implement the ISPS Code* (www.imo.org).

countries of the former Soviet Union and Eastern Europe were described as being slow in implementing the new ISPS security rules.[10]

According to the IMO, national authorities as well as any relevant industries displayed a pragmatic and reasonable attitude towards parties responsible for the implementation of the new security measures in the weeks following the 1 July deadline. No major disruptions to global trade were reported as a result of non-compliance, and, in particular, a responsible attitude was displayed in cases where administrative bottlenecks were to be blamed for any identifiable shortcomings. Nevertheless, there were some reports of ships being detained, cautioned or turned away.[11]

Overall, it appears that the challenge of ensuring compliance with a wide range of requirements and within a tight timeframe has been remarkably well met by Governments and industry alike. However, it needs to be emphasized that the challenge remains, both for Governments and industry, of maintaining substantive compliance with the new international security regime. The ISPS Code is far-reaching, and the scope of the relevant security requirements is wide. In addition to ensuring compliance with the relevant formal requirements of the Code,[12] both Governments and industry are under a continuous obligation to conduct risk assessments and to ensure that effective and appropriate responses to the identified level of risk are taken.

A number of guidance circulars relating to the implementation of the ISPS Code have been issued by the Maritime Safety Committee (MSC) of the IMO. These include in particular the following:

MSC Circular 1111[13] deals in some detail with the security measures and procedures to be applied at the ship/port interface when either the ship or the port facility do not comply with the requirements of chapter XI-2 and of the ISPS Code.[14]. An Annex provides detailed "*Interim Guidance on Control and Compliance measures to Enhance Maritime Security*".[15]

- MSC Circular 1130[16] contains guidance on security-related information, which must be supplied or may be requested prior to entry of a ship into port.
- MSC Circular 1132[17] provides guidance on a variety of matters, in particular the setting of and response to security levels, the practice of requiring and responding to requests for a declaration of security and matters relevant to access and boarding procedures.

---

[10] See Press Briefing of 6 August 2004, *Security compliance shows continuous improving* (www.imo.org). Regarding ISPS Code compliance by IAPH Member Ports, see the IAPH website (www.iaphworldports.org).

[11] See *Measures to Enhance Maritime Security; Progress Report on the Implementation of the Special Measures to Enhance Maritime Security Detailed in SOLAS chapter XI-2 and the ISPS Code*, MSC 79/5/1, 24 September 2004, paras. 6, 7 (www.imo.org).

[12] Note, for instance, a survey on ISPS Code implementation carried out by the European Seaports Organisation (ESPO), which draws attention to the fact that some ships appear to be presenting tonnage certificates of below 500 GT, issued under pre-1969 Tonnage Measurement Rules, and are thus exempt from the ISPS Code requirements. See *ESPO Survey of implementation of ISPS Code/EU Regulation in EU Ports*, of 8 March 2005 (www.espo.be).

[13] See *Guidance relating to the Implementation of SOLAS chapter XI-2 and the ISPS Code* MSC/Circ. 1111, of 7 June 2004. The guidelines also provide recommendations for ships calling at the port of a State that is not a Contracting Government and remind all parties that the requirement for ships to keep records of their last 10 calls at port facilities applies only to calls made on or after 1 July 2004.

[14] Ibid. Annex 1. The Guidance also addresses the position of ship construction, conversion and repair yards and deals with the requirements of chapter XI-2 and the ISPS Code, when a ship interfaces with a floating production, storage and offloading unit (FPSO) or a floating storage unit (FSU).

[15] Ibid. Annex 2.

[16] MSC/Circ.1130, of 14 December 2004, *Guidance to Masters, Companies and Duly Authorized Officers on the Requirements Relating to the Submission of Security-Related Information Prior to the Entry of a Ship into Port* (www.imo.org).

[17] MSC/Circ.1132, of 14 December 2004, *Guidance relating to the Implementation of Solas Chapter XI-2 and the ISPS Code,* (www.imo.org).

- MSC Circular 1131[18] provides *Interim guidance on Voluntary Self-Assessment by SOLAS Contracting Governments and by Port Facilities*. The guidance contains a questionnaire to allow Governments to assess the effectiveness with which obligations in respect of port facilities are and continue to be fulfilled.

In order to effectively implement the wide range of ISPS Code security requirements, Governments and industry incur significant costs. Attempts have been made to assess the approximate costs involved, both globally and at the national level, but no comprehensive assessment has been published since the ISPS Code entered into force. How costs should be distributed, between Governments and industry and among different parties within the affected industries, remains a matter of debate.

As concerns cost sharing between parties within the affected industries, so far there is a clear trend, particularly among port authorities and terminal operators but also among ship-owning or -operating companies, to pass on the extra costs associated with the new security regime to their customers through the imposition of security fees and charges. While increasingly common, the practice is not yet uniform, and there seem to be considerable variations in the level of charges. While generally accepting the need to recover security costs, shippers are faced with charging practices of both ports and shipping lines that lack transparency and add to transaction costs, particularly for developing-country traders.

For instance,[19] terminal security fees quoted for continental European ports range from around €2 per container (import and export container, excluding trans-shipment) for Oslo to around €5 for several Spanish ports, €8 for most Italian ports, €8.50 for Rotterdam and €9 for Bremerhaven, Hamburg, Le Havre, Antwerp and Zeebrugge. Charges quoted for UK ports range, for export containers, from £4.75 in Thamesport to £7.50 in Felixstowe and, for import containers, from £5.50 in Southampton to £10.50 in Felixstowe. Similar variations may be observed in other parts of the world.[20]

Security charges introduced by some container lines also vary, albeit to a lesser extent. For instance, the Far Eastern Freight Conference (FEFC) announced in August 2004[21] that its members would charge €5 for containers "moved to or from ports in the North Continent of Europe, Scandinavia, the Baltic and the Mediterranean", £1.50 for movements to and from the UK ports of Tilbury, Felixstowe, Southampton and Thamesport (where lines recover the security charge from shippers/consignees), and £3.50 for movements to and from other UK ports. Hapag-Lloyd Container Line charges a "carrier security fee" of $6 per container,[22] and P&O Nedlloyd announced in December 2004 that it would charge a $6 carrier security charge on all containers handled by the line from 1 January 2005.[23] "

---

[18] See *Interim guidance on voluntary self-assessment by SOLAS Contracting Governments and by port facilities*, MSC/Circ.1131, of 14 December 2004.

[19] The information in the text is taken from a table compiled by Hapag-Lloyd Container Line providing details of "Terminal Security Fees" applicable in various European, Australian, US, South American and New Zealand ports (www.hlcl.com). An informative and useful summary of port security fees and charges assessed by North American port authorities and terminal operators has been published by the American Association of Port Authorities (www.aapa-ports.org).

[20] Ibid.

[21] See announcement of 13 August 2004 (www.fefclondon.com).

[22] See www.hlcl.com.

[23] See www.ponl.com.

***Review of Maritime Transport, 2006*:**

"Legal Issues Affecting Transportation: An Overview of Recent Developments Relating to Maritime and Global Supply Chain Security, […]

1. Maritime and global supply chain security

Maritime and global supply chain security continues to remain high on the international agenda, and several international organizations are continuing their work to develop standards and recommended practices in these areas. Important international developments in the field include those described below.

In January 2006, a high-level **Ministerial Conference on International Transport Security** was held in Japan.[24] The conference recognized inter alia the serious threat to international maritime transport posed by acts of terrorism, and the continued need to address vulnerabilities. In that connection, it welcomed the activities undertaken by relevant international organizations, particularly the International Maritime Organization and the World Customs Organization,[25] and invited those organizations to consider, in cooperation, the development of appropriate measures to enhance the security of the maritime transport of containers in the international supply chain. In addition, IMO was invited to undertake a study and, as necessary, make recommendations for enhancing the security of ships other than those already covered by SOLAS Chapter XI-2 and the ISPS Code.[26] States were urged to ensure the continued compliance of their port facilities with the requirements of SOLAS Chapter XI-2 and the ISPS Code. Furthermore, it was resolved to share best practices in the implementation of those instruments, to continue to provide assistance and support for capacity building, and further promote international cooperation in the education and training of officers.

In relation to international supply-chain security, a major development was the unanimous adoption in June 2005 of *The Framework of Standards to Secure and Facilitate Global Trade*[27] *(SAFE Framework)* by the Council of the **World Customs Organization**.[28] The SAFE Framework rests on two "pillars", namely Customs-to-Customs Network arrangements and Customs-to-Business partnerships, and consists of four core elements:

1. The Framework harmonizes the advance electronic cargo information requirements concerning inbound, outbound and transit shipments.
2. Each country that joins the Framework commits itself to employing a consistent risk management approach to address security threats.
3. The Framework requires that at the reasonable request of the receiving nation, based on a comparable risk-targeting methodology, the sending nation's Customs administration will perform an outbound inspection of high-risk containers and cargo, preferably using non-intrusive detection equipment such as large-scale X-ray machines and radiation detectors.

---

[24] The Conference was held in Tokyo on 12 and 13 January 2006. The objective was to exchange views and information on international transport security in the aviation, land and maritime sectors, and to discuss the issues that should be addressed in an internationally coordinated and cooperative manner. For further information, see http://www.mlit.go.jp/english/.

[25] For further details, see *Ministerial Statement on Security in International Maritime Transport*.

[26] The reference relates to amendments to the *Safety of Life at Sea Convention* (SOLAS), 1974, which was adopted in 2002. For information on this, see the IMO website at www.imo.org. See also UNCTAD*, Review of Maritime Transport 2005*, p. 84.

[27] For more information see www.wcoomd.org.

[28] At that time, the WCO was composed of 166 member States. At the time of writing, that number had risen to 169.

4. The Framework defines the benefits that Customs will provide to businesses that meet minimal supply-chain security standards and best practices.

The *SAFE Framework* relies on modern Customs principles contained in the revised Kyoto Convention,[29] which entered into force in February 2006, such as risk management based on advance electronic information, use of modern technology and a partnership with trade. It is based on existing supply-chain security and facilitation initiatives and programmes already in place at national levels, for example and in particular, in the United States.

Implementation of the Framework is intended to help Customs authorities to enhance their risk-assessment and risk-management capabilities and adopt an intelligence-based selective approach to targeting closed containers for inspection, primarily on the basis of advance electronic information provided by economic operators involved in the international supply chain. It is designed to improve Customs authorities' abilities to detect and deal with high-risk consignments before their arrival, and thus increase efficiency in the administration of goods by reducing their clearance and release time.

The *SAFE Framework* establishes the concept of the "Authorized Economic Operator" (AEO), who is involved in the trade supply chain and is approved as meeting certain criteria broadly outlined in the standards of the Customs-to-Business pillar of the Framework (Annex 2). Such operators should be entitled to participate in simplified and rapid procedures for the provision of minimum information. Detailed implementation requirements for the *SAFE Framework*, including those for cargo security and for AEOs, are being drawn up by the WCO.

As of June 2006, 135 WCO members had expressed their intention to implement the Framework. Many of those members will require capacity building. In order to assist developing countries in particular in the implementation of the *SAFE Framework*, the WCO's Directorate for Capacity Building has recently launched a major capacity-building programme, known as COLUMBUS, under which diagnostic missions are conducted, a needs assessment is carried out and an action plan is developed, with a view to identifying donors that are willing to fund projects to enable Customs Administrations to become *SAFE Framework* compliant.[30] At present, it is not possible to adequately assess the trade-related impacts of the implementation of the new global supply-chain security framework. Much will depend on whether SMEs, particularly in developing countries, will be able to comply with the requirements, such as those related to the use of electronic communication and modern technology and those related to AEO recognition, and on whether mutual recognition of the AEO status can effectively be achieved.

The idea of a voluntary framework for the recognition of "secure operators" is also under discussion at the level of the **European Union**. Recently, a Communication[31] was issued by the European Commission, containing a proposal for an EC Regulation to introduce a voluntary security scheme under which operators in the supply chain would increase their security performance in exchange for incentives, such as fast-track treatment both inside the EU and at external borders, and obtain "secure operator" status. For this purpose, member States might either avail themselves of existing systems or procedures or create a specific system for supply-chain security. The scheme would cover intermodal transport and follow previous terrorism legislation in the field of maritime

---

[29] *International Convention on the Simplification and Harmonization of Customs Procedures (as amended),* June 1999.

[30] See the Speech by the Deputy Secretary General of the WCO at the 11th WCO Asia Pacific Regional Heads of Administration Conference, 4 April 2006, Beijing China (www.wcoomd.org).

[31] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on enhancing supply chain security, *Proposal for a Regulation of the European Parliament and of the Council on enhancing supply chain security*, COM(2006), 79, 27 February 2006.

transport and ports. To obtain "secure operator" status, an operator would have to implement a security management system and demonstrate that it covers areas such as protection of buildings, access control and personnel procedures. As with the requirement of the WCO *SAFE Framework*, each member State would have to recognize the "secure operator" status conferred by another member State.

It should be noted that the **International Maritime Organization** (IMO) has begun to consider proposals for integrating, into international legislation,[32] appropriate cargo security procedures based on or compatible with the standards of the WCO's *SAFE Framework* Thus, key elements of the WCO standards may in due course become part of the international law for maritime cargo transports, such as the 1965 *Convention on Facilitation of International Maritime Traffic* (FAL), as amended, and the 1974 *Safety of Life at Sea Convention* (SOLAS), as amended.

Amendments to SOLAS, which were adopted by the IMO in 2002, including in particular the *International Ship and Port Security* (ISPS) *Code*, continue to represent the most important international set of rules for the security of ships and port facilities.[33] The ISPS Code entered into force on 1 July 2004, and the IMO's Maritime Safety Committee (MSC) has issued a number of guidance circulars to assist in the implementation of and compliance with the requirements of ISPS Code.[34] Most recently, at its 81st session in May 2006, the MSC adopted a further set of guidance circulars,[35] notably the following:

MSC.1/Circ.1192, Guidance on voluntary self-assessment by SOLAS Contracting Governments and by port facilities;[36]

MSC.1/Circ.1193, Guidance on voluntary self-assessment by Administrations and for ship security;

MSC.1/Circ.1194, Effective implementation of SOLAS chapter XI-2 and the ISPS Code.

In relation to the ISPS Code, it should also be noted that the **UNCTAD** secretariat is in the process of conducting a large-scale survey that seeks to establish the experiences and views of parties directly affected by the new maritime security regime, especially as regards costs related to the implementation of the ISPS Code. These parties include Governments, shipowning and operating

---

[32] See *Enhancement of security in cooperation with the WCO,* doc. MSC/81/5/4, 9 February 2006. See also *Measures to Enhance Maritime Security*, Report of the Working Group on Maritime Security (Part I), MSC 81/WP.5, of 17 May 2006. The Maritime Safety Committee (MSC), at its 81st session, in May 2006, discussed the carriage of closed transport units and of freight containers transported by ships and referred the matter to the Ship/Port Interface (SPI) Working Group of the Facilitation Committee for further consideration, including the development of draft amendments to the SOLAS Convention.

[33] For an overview over the responsibilities of Governments, port facilities and ship-owning and ship-operating companies under the ISPS Code, see UNCTAD, *Container Security: Major Initiatives and Related International Developments*, UNCTAD/SDTE/TLB/2004/1, paras. 80–86. See also *UNCTAD Review of Maritime Transport 2005*, p. 84.

[34] The MSC circulars are available on the IMO website (www.imo.org). See also UNCTAD, *Review of Maritime Transport 2005*, p. 87.

[35] Other circulars adopted include MSC.1/Circ.1188, *Guidelines on training and certification for port facility security officers*; MSC.1/Circ.1189, *Guidance on the provision of information for identifying ships when transmitting ship security alerts*; MSC.1/Circ.1190, *Interim scheme for the compliance of special purpose ships with the special measures to enhance maritime security*; and MSC.1/Circ.1191, *Further reminder of the obligation to notify flag States when exercising control and compliance measure.* A full list of all relevant circulars is included in MSC.1/Circ.1194.

[36] The Guidance circular is a revised version of MSC/Circ.1131.

companies engaged in international transport, and ports serving such ships. The results of the survey are expected to be available by the end of 2006.[37]

With regard to other relevant developments at **IMO**, it is also worth drawing attention to progress in relation to the introduction of *Long-Range Identification and Tracking Systems* (LRIT). By way of background, it should be recalled that it is already a special mandatory SOLAS requirement[38] for certain categories of ships to be equipped with *Automated Identification Systems* (AIS). AIS are shipboard automatic electronic reporting devices that communicate basic information regarding the ship's identity, position, course and speed to other AIS transponders and shore-based facilities. The AIS currently used are capable of transmitting information up to a range of around 50 nautical miles offshore. In order to extend significantly the tracking capabilities of SOLAS Contracting Governments, the introduction of LRIT has been proposed.

After extensive discussions,[39] the MSC adopted in May 2006 new regulations for the LRIT, to be included in SOLAS chapter V (Safety of Navigation), together with associated performance standards and functional requirements.[40] The MSC also approved the establishment of an ad hoc Working Group on Engineering Aspects of LRIT.

LRIT will be a mandatory requirement for ships engaged in international voyages, more particularly passenger ships (including high-speed craft), cargo ships (including high-speed craft) of 300 gross tonnage and upwards, and mobile offshore drilling units. The SOLAS regulation establishes a multilateral agreement for sharing LRIT information among Contracting States on the identity, location, date and time of the position of ships for security and search and rescue purposes. It maintains the right of flag States to protect information about ships flying their flag, as appropriate, while permitting coastal States access to information about ships navigating up to 1,000 nautical miles off their coasts.[41] While AIS is a broadcast system, data derived through LRIT will be available only to recipients who are, according to the regulation, entitled to receive the information.[42] Safeguards concerning the confidentiality of data have been built into the relevant regulatory provisions. The regulation provides for a phased-in implementation schedule for ships constructed before its expected entry into force date of 1 January 2008, as well as some exemptions for ships operating exclusively in certain areas and already fitted with AIS.

Efforts are also being made at **IMO** to incorporate security-related provisions into other international legal instruments, such as the 1978 *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers* (STCW Convention) and the STCW Code.[43]

---

[37] Information on results of another survey conducted by the International Transport Workers' Federation (ICFTU), bringing to the attention of the MSC, inter alia, problems experienced by seafarers in obtaining shore leave following the implementation of the ISPS Code, can be found in IMO document MSC 81/5/8, submitted for consideration at the 81st session of the MSC (10–19 May 2006).

[38] SOLAS chapter V/19.

[39] The issue of LRIT has been considered by the Maritime Safety Committee (MSC) and by the Sub-Committee on Radiocommunications and Search and Rescue (COMSAR). For further information, see most recently the COMSAR Report to the Maritime Safety Committee (COMSAR 10/16, section 10, also published as an extract in document MSC 81/5/Add.1, and Annexes 17 and 18) and *Measures to Enhance Maritime Security*, Report of the Working Group on Maritime Security (Part II), MSC 81/WP.5/Add.1. See also the IMO website (www.imo.org).

[40] Resolutions MSC.202(81), MSC.210(81) and MSC.211(81).

[41] Note that it has been emphasized that the regulation "was not creating or affirming any new rights of States over ships beyond what was existing in international law, particularly UNCLOS, nor altering existing rights, jurisdictions, duties and obligations of States in connection with the law of the sea"; see the note by the Secretary-General for consideration by the Council at its 96th session, document C 96/7/Add.1 of 30 May 2006.

[42] While the costs arising for States seeking to receive LRIT information are, at this stage, not yet clear, some reference to various likely charges is provided in COMSAR 10/16 (MSC 81/5/Add 1), at para. 10.50.

[43] For an overview of other amendments to SOLAS and mandatory codes and guidelines adopted by the MSC at its 81st session in May 2006, see the IMO website (www.imo.org).

Finally, it should be noted that amendments to the 1988 *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation* (SUA Convention)[44] and its 1988 Protocol[45] were adopted on 14 October 2005 under the auspices of IMO. Once widely and uniformly implemented by IMO States Parties, the 2005 SUA Protocols[46] will provide a legal basis for the arrest, detention and extradition of persons in the event of a terrorist attack against shipping. The main amendments effected by the 2005 Protocols include the following:

A broadening of the list of offences already contained in the 1988 SUA Convention and its Protocol. The offences listed shall be made punishable by each State Party by appropriate penalties that take into account their gravity.
Inclusion in the 1988 SUA Convention of provisions covering cooperation and procedures to be followed if a State Party desires to board on the high seas a ship flying the flag of another State Party, when the requesting party has reasonable grounds to suspect that an offence under the Convention has been or is about to be committed. The authorization of the flag State is required before such boarding.
Inclusion in the 1988 SUA Convention of a provision to the effect that none of the offences should be considered a "political offence" for purposes of extradition, and of a provision dealing with conditions under which a person detained may be transferred to another State Party.[47]
The Protocols were opened for signature on 14 February 2006 and will remain open for signature until 13 February 2007. Thereafter they will remain open for accession. Seventy-one States signed the Final Act of the Conference.[48]"

- - - - -

[44] *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation,* 1988 (SUA Convention).
[45] *Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf,* 1988 (SUA Protocol).
[46] 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988 (SUA Convention); and 2005 Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 1988 (SUA Protocol).
[47] For further information, see the IMO website, www.imo.org.
[48] The 2005 Protocol amending the SUA Convention requires adoption by 12 member States to enter into force. The 2005 Protocol to the SUA Protocol requires adoption by only 3 State Members, but its entry into force is contingent on the entry into force of the amendments to the SUA Convention.