

FOURTH REGULAR SESSION  
January 28 -30, 2004  
Montevideo, Uruguay

OEA/Ser.L.X.2.4  
CICTE/INF.5/04  
29 January 2004  
Textual

#### ALTERNATIVE SOURCES OF FINANCING FOR SECURITY IMPROVEMENTS

(Presentation by Sheila M. Donovan, Director, Department of Development Programs  
OAS Inter-American Agency for Cooperation and Development)

## ALTERNATIVE SOURCES OF FINANCING FOR SECURITY IMPROVEMENTS

(Presentation by Sheila M. Donovan, Director, Department of Development Programs  
Inter-American Agency for Cooperation and Development)

Thank you, Mr. Chairman, for giving me and the agency I represent the opportunity to address this fourth plenary session on the issue of alternative sources of financing for security improvements -- an issue that is essential not only for security in the hemisphere and so many other hemispheric priorities, among them defense, transportation, infrastructure and perhaps most especially trade.

Member countries' immediate challenge is to comply with the provisions of the ISIP (International Ship and Port Facilities Security Code) by July 1, 2004. I will speak at this point only to the issue of Port security. However, almost all of my comments regarding alternatives for financing also apply to airport security enhancements. In fact, many airports around the world are old hands at utilizing imaginative and innovative combinations of financing sources.

Returning to the specific issue of port security, perhaps the most important point to make at the outset is that the principal point of reference and accountability for the new security measures mandated in the ISPS code falls squarely on the National Governments who are members of the IMO (International Maritime Organization) and signatories to the code and related conventions.

The ISPS code contains detailed, security-related requirements for governments, port authorities, and shipping companies in a mandatory compliance section (Part A), together with a series of guidelines about how to meet these requirements in a second section (Part B). The code addresses the need for risk management, and it endeavors to ensure the security of ships and port facilities through the application of security plans based on the outcomes of the risk assessment.

A useful document issued by the Inter-American Ports Committee and the US Maritime Administration (MARAD), "Guide to Understanding and Implementing the ISPS Code" is available on the websites of both MARAD and the CIP.

I would like to briefly mention some of the most important elements of the ISIP:

First, Contracting Governments have an obligation to designate a National Command Authority, which has the overall responsibility to undertake a full range of steps to comply with ISPS. It must also establish a framework for cooperation between government agencies, local administrations and the shipping and port industries. The authority is also called upon to determine roles and responsibilities for those entities in assuring maritime security at the national and international levels.

A port facility security, or risk, assessment is required for all ports in the national territory. The assessment is to be designed to evaluate the security in accordance with the ISPS, and must be periodically reviewed and updated. The assessment must include, at a minimum, the following elements:

- Identification and evaluation of important assets and infrastructure;
- Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;
- Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability; and
- Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

The next requirement, which builds on the risk assessment, is the development of a port facility security plan for each port facility, which must be approved by the contracting government.

- A Port Security Officer must be designated for each port facility – can cover multiple port facilities.

## IMPLICATIONS

Many ports in the hemisphere will already be essentially compliant with the requirements of the code; many others, however, will require varying degrees of effort and resources – human, technical, financial – to comply. In addition, even those large, well managed and well funded ports will very likely find gaps in their security that will have to be filled. Training and capacity building will remain a challenge for all. And there are other elements that while not as urgent in terms of timing, are certain to arise – primarily connected with ensuring security in the supply chain – for all trading partners. In the US, as in many other Member States, there are currently several government initiatives aimed at developing best practices and standards for use by commercial maritime shippers, including the Transportation Security Administration's Operation Safe Commerce, the Custom Department's Custom Trade Partnership Against Terrorism and Container Security Initiative, and USDOT's Intelligent Transportation. There would seem to be no doubt that new standards and requirements instituted by all Member States for trading partners will affect all the links in the supply chain, and that compliance with those standards will be absolutely necessary in order to remain competitive and secure.

More immediately, the US Marine Transportation Act of 2002 requires the US Coast Guard to assess the effectiveness of anti terrorism measures maintained at foreign ports, and to notify foreign authorities if those measures are not effective, and exercise control over vessels, including prescribing conditions of entry or denial of entry into a US port.

## FINANCING OPTIONS/ALTERNATIVES

Compliance with ISPS is the most urgent matter, and will most likely have to be paid for from current budgets or technical assistance programs, given the short time frame. The Inter American Ports Committee, along with US MARAD, is sponsoring a Hemispheric Conference on Port Security next month in Miami (February 25-27), one of whose objectives is to identify the budgetary requirements of OAS member states to establish and maintain a high level of security within the marine transportation system in the hemisphere. It also will seek to help the neediest ports comply with the new standards. The latter will probably be achieved through identification of non reimbursable resources or other technical assistance that could be applied immediately to those in most need.

It is the next steps that will likely require the most resources. That is, once the gaps, risks and needs are identified, solutions will be worked out and along with the solutions, financing must be sought and secured to pay for their implementation. Indeed, keeping risk assessments and security plans current and tested will in itself require substantial ongoing funding. And as noted just now, we can anticipate the need for large investments in the future to enhance the security of the entire supply chain.

Generally speaking, needed security improvements that derive from compliance with ISPS and other circumstances can be funded through a combination of funding sources, including national budgets, user fees, international financial institution support, IDB and World Bank loans, and private sector participation. However, the establishment enabling legislation, regulation and rules may be necessary in many cases. Even when new legislation or regulation is not required, the introduction of some revenue-producing schemes could result in complex legal, commercial and competitive challenges.

It is not realistic to rely on any one sector or any one source to provide the funds necessary. Therefore it is essential that policy makers, legislators, local authorities and the private sector work together to “think outside the box.” For example, given the connectedness of national transportation systems – intermodal everywhere now – funds derived from other transportation fees or taxes could be “shared” with ports in order to provide a portion of the funds required for security enhancements. This could be achieved through the provision of a “set aside” of a certain percentage of fees or taxes collected throughout the national transportation system for certain intermodal freight projects which would help to fund security needs at ports.

User fees (often otherwise known as taxes) are another widely used source of funding. Each Member State, however, will need to explore the implications of applying fees at a national level – once again, because of probable legal, regulatory and competitive challenges – or at a local level, either by port authorities, municipal or state. A very important challenge here is to prevent the fees from going to a general purpose trust fund; rather, the utilization of fees collected should be restricted to a specific purpose, project and/or initiative.

Customs duties: a portion of customs duties collected at each port of entry could be returned directly to that port as an entitlement to be used for security enhancements.

Longer term financing possibilities for security enhancements as well as other capital expenditures include:

- a. Private sector participation in ports. During the 1990's, many countries in our region – Argentina, Mexico, Panama, the Bahamas, Brazil, Colombia, Jamaica – had transferred control of port facilities to the private sector. There are several types of private sector involvement in ports:
  - i. Operations and management, whereby the private sector entity takes over management of a state-owned enterprise for a given period. Includes management contracts and leases.
  - ii. Operations and management with capital expenditures. In this case, the private sector enterprise assumes significant investment risk.
  - iii. Greenfield projects, where a private sector enterprise builds from scratch and operates a new facility, again with substantial capital investment on the part of the private sector firm.

Most of the private port operators take on large investment obligations for expansion and modernization of existing facilities. These are generally structured as concessions, not divestitures of assets by the governments. The concession model is in many respects tried and true, and can be adapted easily to a smaller scale, limited scope operation. There are many private sector companies that will provide turn-key, customized solutions for these facilities, with no upfront investment by the port, airport or country, and can provide follow up service, including back office, training, operations, back up and monitoring. Airports in Europe especially have some excellent experience in concessioning services, including security services, to private companies.

The international financial institutions – IDB and World Bank – are working on using some less conventional instruments to help national governments fund their general infrastructure needs. For example, both IDB and World Bank discussed using financial guarantees from those institutions to back debt placements on capital markets, or to guarantee member states' contingent liabilities, which would substantially decrease the overall cost to the country of funding this type of project.