APEC International Ship and Port Facility Security Code Good Practices Workshop

Summary Proceedings

Sydney, Australia, October 2-3, 2013

APEC Maritime Security Sub-Group
APEC Transportation Working Group

November 2013

APEC Project TPT 10/2012A

Produced by
John Platts
Ottawa, Canada
11 November 2013

For
Asia Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#213-TR-01.4

Executive Summary

The APEC International Ship and Port Facility Security (ISPS) Code Good Practices Workshop was held in Sydney, Australia from 02 to 03 October 2013. It was hosted by Australia's Department of Infrastructure and Regional Development in collaboration with APEC's Maritime Security Experts Group, the International Maritime Organization's (IMO) Maritime Safety Division and the Organization of American States' (OAS) Inter-American Committee on Counter-Terrorism.

The workshop's objective was to identify and share good practices in port security oversight linked to implementing the ISPS Code by discussing the lessons learnt from APEC's recently-ended Port Security Visit Program and other regional capacity building initiatives as well as opportunities to broaden the scope of the ISPS code's application within port areas. The workshop was the first of its kind within the Region and provided a unique opportunity for the national authorities responsible for port security to not only take stock of their progress in implementing the ISPS Code almost 10 years after it took effect but also to explore ways of coordinating efforts to address region-wide port security issues and challenges on an ongoing basis.

The workshop was attended by a senior official from the authority of eight (8) Economies, all of which had participated in the PSVP or hosted a similar visit from the IMO. The workshop's format enabled a preliminary list of 17 good practices and set of seven (7) recommendations to be identified for further consideration. However, the wide range of topics that were discussed over a two day period did not provide sufficient time for the outcomes and their underlying rationale to be refined. Also, it was recognized that, as they were derived by the representatives of just eight APEC Economies, they may not fully reflect the collective views of the Designated Authorities in the region. Nevertheless, the participants were satisfied that the results of the workshop should provide a strong foundation for further discussions in connection with future capacity-building initiatives linked to ISPS Code implementation.

ISPS Code Good Practices Workshop (IGPW)

1. Background

Following the termination of the Port Security Visit Program (PSVP) in 2011, the concept of a workshop to build on its findings was endorsed by APEC's Maritime Security Sub-Group (MEG-SEC) in July 2012. The initiative was transformed into a project proposal which was approved by the APEC Secretariat in December 2012. Australia, one of the 12 APEC Economies which had participated in the PSVP, agreed to host the workshop.

2. Objective

The IGPW's objective is for the authorities in APEC Economies which had been involved with the PSVP to share good practices in port security oversight linked to implementing the ISPS Code by:

- Collectively taking stock of their progress in implementing the ISPS Code almost 10 years after it took effect;
- Discussing lessons learnt from the PSVP and other regional capacity building initiatives including the post-PSVP specialized workshops that have been funded under APEC's ongoing ISPS Code Implementation Assistance Program (which is also under the general direction of MEG-SEC);
- Identifying opportunities to broaden the scope of the ISPS Code's application within port areas; and
- Exploring ways to address region-wide port security issues and challenges on an ongoing basis.

3. Approach

3.1 Participation

In order for the discussion-oriented workshop to run successfully, it was necessary to restrict participation to one senior official from the national authority responsible for port security in each APEC member economy which participated in the PSVP or had hosted a similar visit from the IMO. Initially, letters of invitation were sent to 15 Economies of which 11 indicated their acceptance. Unfortunately, due to unforeseen circumstances, representatives from three of these economies were unable to attend, thereby reducing workshop participation to representatives from Australia, Brunei Darussalam, Indonesia, Republic of Korea, Mexico, Peru, the Philippines and Thailand and (see Appendix A for details).

3.2 Discussion Topics

Following a review of the summary reports prepared after each PSVP visit, 13 topics were selected for discussion under two themes:

- Strengthening port facility oversight programs
- Strengthening port security frameworks

A topic dedicated to security training was separately identified as it was common to both themes. In addition, a short visit to the Overseas Passenger Terminal at Sydney Harbour was arranged which allowed participants to discuss implementation practices with the PFSO. These included the importance of maintaining a good working relationship with major industry stakeholders (e.g. cruise ship operators) in dealing with the complexities of the terminal being located in a busy port environment with significant operational constraints.

The topics are listed in the final agenda which is shown in Appendix B. To facilitate discussion:

- reference sheets were prepared for each topic identifying ISPS Code requirements, guidance material available for Designated Authorities and possible discussion points;
- participants were invited to make short verbal presentations on their experiences; and

- supplementary material was provided by two Designated Authorities as an example of their good practices with respect to particular topics.

Due to the 2-day length of the workshop, it was necessary to limit discussion on each topic. The discussions reflected the differences of the participants both in terms of the scope of their responsibilities for port facility security (two participants were not located in their Designated Authority) and how the ISPS Code is being implemented within their government's broader framework for maritime security. For this reason, the outcomes identified below were considered to be preliminary and in need of refinement. However, they reflect the consensus of the participants and are sufficiently robust to provide a strong starting point for future discussions.

4. Outcomes

In addition to enabling an informal regional network to be established among senior officials within national authorities responsible for port facility security, the workshop achieved two main outcomes:

- The identification of a preliminary list of good practices in port security oversight, for consideration by Designated Authorities; and
- A preliminary set of recommendations on future capacity building initiatives, for consideration by the workshop sponsors to table at the next MEG-SEC meeting.

4.1 Identification of good practices in strengthening port facility security oversight programs

The 10 practices linked directly to the strengthening of port facility security oversight programs which were identified by the participants are listed in the table below along with the reasons for their selection.

Identified Good Practices	Rationale
4.1.1 Recognizing cyber-security as an important threat when updating Port Facility Security Assessments (PFSAs).	This is not one of the security incidents listed in section B15.3 of the ISPS Code, 2003 Edition.
4.1.2 Adapting a risk-based approach to determining the frequency of intermediate audits of Port Facility Security Plans (PFSPs) conducted by Designated Authorities or their authorized Recognized Security Organizations (RSOs).	This practice assumed that PFSPs would be subjected to an audit every five years as a condition of renewing their Statements of Compliance.
4.1.3 Requiring PFSOs to maintain a manual of port facility security procedures	Although not specified in section A17.2 of the ISPS Code, 2003 Edition, the set of 13 requirements for PFSOs imply the need for such a manual.
4.1.4 Establishing specific time periods for when Occasional Use Facilities and the SOLAS ships using them must be ISPS Code-compliant	Although section A3.2 of the ISPS Code, 2003 Edition, requires Designated Authorities to decide on the extent to which the Code applies to those port facilities which occasionally serve ships arriving or departing on international voyages, no guidance is provided on how to make this determination other than to base the decision on the results of a PFSA.
4.1.5 Requiring secure control rooms to be a mandatory feature at all ISPS Code-compliant port facilities	Whereas section A9.4 of the ISPS Code, 2003 Edition, *requires* Ship Security Plans to identify restricted areas on board SOLAS ships, section B16.21 only *recommends* their identification at port facilities.
4.1.6 Developing public awareness products to show the port security role of Designated Authorities	While there is industry awareness of the role of Designated Authorities and other government organizations in implementing the ISPS Code and of the importance of

	security measures, in general there is a much lower level of awareness for the public, notably people living in communities adjacent to port areas or local businesses which provide services to port facilities and their personnel. As a result, a major challenge facing many Designated Authorities is to develop awareness campaigns that promote an effective security culture encompassing both the port industry and the public.
4.1.7 Adopting a multi-layered approach to planning exercises on a regular basis	Section A18.4 of the ISPS Code, 2003 Edition, requires PFSOs to participate in exercises "at appropriate intervals". Section B18.6 recommends that exercises should be carried out at least once each calendar year with no more than 18 months between exercises. The Code does not require PFSOs to plan, conduct and evaluate exercises. As indicated by its title, the APEC Manual of Maritime Security Drills and Exercises for Port Facilities, Version 2, June 2012, was designed to provide guidance on the planning, conduct and evaluation of live and table-top exercises at the port facility level. Increasingly, Designated Authorities, in coordination with other government organizations, are assuming responsibility for the planning, conduct and evaluation of exercises. In some cases, these have been at the port level; in others, they have involved multiple ports within a SOLAS Contracting Government. Occasionally, they have involved the ports of multiple Contracting Governments.
4.1.8 Providing non-confidential information to stakeholders on threats and risks	Although the detail and type of information would vary between Economies based on the determination of their national security organizations, such a practice was considered beneficial in raising the level of security awareness among stakeholders.
4.1.9 Allowing alternative security measures that are proportionate and flexible	Although Regulation 12 of SOLAS Chapter XI-2 and section B4.27 of the ISPS Code, 2003 Edition, provides for Designated Authorities to allow port facilities to implement security measures that are equivalent in their effectiveness to those prescribed in the ISPS Code, no guidance exists as to what these might be. Such arrangements (e.g. the use of barking dogs in lieu of fences) could be effective in the case of quays attached to factories with infrequent operations.
4.1.10 Having standard operating procedures for reporting security incidents	The discussion revealed significant variation in incident reporting procedures. In some cases, reporting is voluntary while in others it is mandatory. It was also noted that PFSOs may be reluctant to report incidents as they consider the information to be proprietary and confidential; also they may not distinguish between security lapses and incidents including those that are 'near misses'.

4.2 Identification of good practices in strengthening port security frameworks

The five practices linked directly to the strengthening of port security frameworks which were identified by the participants are listed in the table below along with the reasons for their selection.

Identified Good Practice	Rationale
4.2.1 Establishing a mandatory requirement for Non-SOLAS facilities to have simplified PFSAs and PFSPs	The ISPS Code and the IMO's related Guide to Maritime Security and the ISPS Code, 2012 Edition contain no guidance on when to develop simplified PFSAs and PFSPs or how they should be simplified. Such a practice was considered to be especially beneficial if adopted by the four Economies comprising the East ASEAN Growth Area.
4.2.2 Requiring all port workers to have identity cards	Although this is neither a mandatory nor recommended requirement in the ISPS Code, it is a standard access control feature of most, if not all, PFSPs. However, not all port administrations are required to develop port-wide security plans and hence workers in port areas other than designated port facilities may not be required to carry identity cards.
4.2.3 Extending the scope of the ISPS Code to encompass non-SOLAS facilities	As SOLAS Contracting Governments enter the final stages of implementing the ISPS Code, consideration is being given to extending the scope of the ISPS Code to facilities serving non-SOLAS vessels. Section 2-18 of the IMO Guide to Maritime Security and the ISPS Code, 2012 Edition identifies the types of non-SOLAS vessels being covered by the ISPS Code. However, no experience-based guidance is available to national authorities wishing to expand the scope of the ISPS Code to cover such non-SOLAS vessels as Floating Production and Storage Offloading (FPSO) vessels, Mobile Off-shore Drilling Units (MODUs), port service providers and vessels servicing off-shore platforms.
4.2.4 Requiring port administrations to establish Port Security Committees	Guidance is available to port administration wishing to establish port-wide security committees in section 3.9 of the IMO Guide to Maritime Security and the ISPS Code, 2012 Edition. These committees are distinct from similar committees that may be established at individual port facilities within the port areas by port facility operators.
4.2.5 Holding annual port security conferences for industry stakeholders	This practice was considered to be an efficient and effective way for Designated Authorities to engage in an open two-way exchange of information with their primary stakeholders including port administrations and port facility operators.

4.3 Security training in support of port security oversight

The two practices linked directly to the provision of security training in support of port security oversight which were identified by the participants are listed in the table below along with the reasons for their selection.

Identified Good Practice	Rationale
4.3.1 Training Compliance Inspector/Officers to have a secondary security promotions role	There is no IMO Model Course for the Designated Authority's counterpart to PFSOs. Hence the role of their compliance inspectors/officers is determined by their Designated Authority. That determination is typically influenced by their regulatory powers in dealing with non-compliance incidents.

	Nevertheless, given the general recognition that non-compliance should be addressed in a fair and proportionate way, it should be possible to promote a secondary security promotion and education role without compromising their primary compliance duties especially when dealing with minor incidents of non-compliance.
4.3.2 Supplementing basic training with On-the-Job training	While PFSOs and other port facility personnel have access to the IMO Model Courses, it was recognized that security officials in Designated Authorities are dependent on the internal courses that may be available or the basic training provided in the IMO's Model Course 3.21, 2011 Edition for PFSOs. In either case, it was considered beneficial for compliance officers/inspectors to have follow- on training by either shadowing experienced personnel in another Designated Authority or being mentored by an expert from another Designated Authority or international organization.

4.4 Recommendations for future capacity-building initiatives

The seven recommendations linked directly to the 17 practices identified above which were identified by the participants are listed in the table below along with the reasons for their selection.

Recommendation	Rationale
4.4.1 Development of standardized checklists covering key PFSO responsibilities	This recommendation arose from concerns surrounding the PFSO's responsibilities in connection with updating PFSAs; conducting internal audits of PFSPs; maintaining an incident reporting system; evaluating the results of drills; and training other port facility security personnel. These checklists could form part of a manual of port facility security procedures identified as a good practice in paragraph 4.1.3 above.
4.4.2 Provision of IMO guidance on the size of maritime exclusion zones when SOLAS ships are berthed at port facilities	The lack of guidance and the variability in the practices of the national authorities represented at the workshop gave rise to this recommendation.
4.4.3Provision of assistance to Designated Authorities in translating the APEC Manual of Maritime Drills and Exercises for Port Facilities, 2nd Edition, 2012 into local languages as well as refining the Spanish translation	Although English is the common language among APEC Economies, it was recognized that not all PFSOs have sufficient linguistic capabilities to be comfortable in using the manual as a reference document, especially for drills. Also, it was noted that the Spanish version contains inaccuracies which has limited its use in the three primarily Spanish-speaking Economies.
4.4.4 Development of simplified exercise scenarios to complement those in the APEC Manual for Maritime Security Drills and Exercises for Port Facilities, 2nd Edition 2012.	The recommendation reflected concern that some Designated Authorities may consider the existing exercise scenarios in the manual to be either not relevant or too complex for their needs and were starting to develop their own scenarios.
4.4.5 Provide guidance on the range and selection of security assessment techniques when updating PFSAs.	It was noted that neither the Guide to Maritime Security and the ISPS Code, 2012 Edition provides guidance on a single assessment technique (which was originally developed for non-SOLAS vessels and facilities by the IMO and issued as Maritime Safety Committee Circular MSC.1/Circ.1283 in December 2008), nor the Port Security Risk Assessment Technique courses (which are currently being delivered

	under APEC's ISPS Code Implementation Assistance Program) link the size and complexity of a port facility to a particular technique.
4.4.6 Develop a standardized maritime security audit manual and course for Designated Authorities.	This recommendation was based on the experience-based observation that different external audit practices may lead to inconsistencies in the oversight of ISPS Code implementation and renewal of Statements of Compliance at port facilities within the APEC Region. Such a manual would provide a standard set of guidelines, procedures and checklists which could be customized as required by Designated Authorities in APEC Economies.
4.4.7 Establish and maintain a Good Practices website	This recommendation is intended to provide a link to the good practices identified in the three preceding sections (4.1-4.3). Such a website could build on the U.S. Coast Guard's Port Security Best Practices site which is based on ISPS Code implementation practices observed during visits to countries currently trading with the United States. As a result, although these practices are international in scope, they tend to be more oriented towards port facility operators than Designated Authorities.

5. Summary

The workshop, which was the first of its kind in the APEC Region, provide a unique opportunity for senior officials in the national authorities responsible for port security to share information and exchange views on matters of mutual interest. The workshop's format enabled a preliminary list of good practices and set of recommendations to be identified for further consideration. However, the wide range of topics that were discussed over a two day period did not provide sufficient time for the outcomes and their underlying rationale to be refined. Also, it was recognized that they were derived by the representatives of just eight APEC Economies, hence they may not fully reflect the collective views of the Designated Authorities in the region. Nevertheless, the participants were satisfied that the results of the workshop should provide a strong foundation for further discussions in connection with future capacity-building initiatives linked to ISPS Code implementation including the conduct of similar workshops.

Appendix A – List of IGPW participants

Economy	Participant	Position & Organization	Designated Authority*
Australia	Steve Dreezer	General Manager, Maritime & Identity Security Branch, Department of Infrastructure & Regional Development	yes
Brunei Darussalam	Lt. Colonel Hj Rizal Fauzan Hj Mohd Bahrin	Head of Maritime Security and Environment Protection, Marine Department	yes
Indonesia	Tri Yuswoyo	Director of Sea & Coast Guard, Directorate General of Sea Transportation, Ministry of Transportation	yes
Republic of Korea	Baek Tae-yeol	General Manager, System Certification Team, Korean Register of Shipping	no
Mexico	Capitan Francisco Javier Bustos Garcia	Unified Center to attend for Maritime Incidents and port, SEMAR-Mexico	no
Peru	Teodoro Aguero Fizcarral	Head of Port Protection, Security & Safety Unit, National Port Authority	yes
The Philippines	Captain Pedro R. Lopez	Chief, Policy Division, Office for Transportation Security, Department of Transportation & Communications	yes
Thailand	Narong Wangdee	Chief of Ship & Port Security, Vessel Traffic Control & Maritime Security Center, Marine Department	yes
APEC	Kelly Edwards	IGPW Project Manager - Pacific Maritime Security Liaison Officer, Department of Infrastructure & Regional Development, Australia	
APEC	John Platts	IGPW Facilitator – Special Advisor, Marine Security, Transport Canada (retired)	

* Source: IMO, Global Integrated Shipping Information System (GISIS), National Authority responsible for port facility security

Appendix B

International Ship and Port Facility Security Code Good Practices Workshop

Sydney, Australia, 02-03 October, 2013

FINAL AGENDA

Day 1 (02 October)

08:30 – 09:00 **Registration**

09:00 – 10:00 **Welcome and Introductions**

- **Host economy opening remarks**
- **Round table introductions**
- **Review of workshop structure:**
  - **Administrative details**
  - **Agenda -** objectives, expected outcomes, topics and timetable
  - **Format –** for each topic, reference sheets and short, verbal accounts by 1 or 2 participants of their economy's authority's experiences as a 'lead-in' for the facilitated discussion
- **Group photograph**

10:00 – 10:30 **Break**

Theme: Strengthening Port Facility Security Oversight Programs [Sessions 1 & 2]

10:30 – 12:30 **Session 1 topics** (approx. 30 minutes per topic)**:**

1.1 Updating Port Facility Security Assessments (PFSAs)
1.2 Inspecting and auditing Port Facility Security Plans (PFSPs)
1.3 Approving PFSA & PFSP amendments
1.4 Addressing non-compliance (enforcement actions)

12:30 – 14:00 **Lunch**

14:00 – 15:00 **Session 2 topics** (approx. 20 minutes per topic):

2.1 Oversight of Occasional Use facilities
2.2 Authorizing Recognized Security Organizations (RSOs) to undertake Designated Authority responsibilities
2.3 Incident reporting techniques

15:00 – 15:20 **Break**

15:20 – 17:00 **Session 3: Visit to Overseas Passenger Terminal at Sydney Harbour:**

- Includes the opportunity for Questions & Answers with the Port Facility Security Officer on implementation challenges and good practices

End of Day 1

Day 2 (03 October)

09:00 – 09:20 **Session 4**: Recap of preliminary findings from Day 1

Theme: Strengthening Port Security Frameworks [Sessions 5 & 6]

09:20 – 10:40 **Session 5 topics** (approx. 20 minutes per topic):
- 5.1 Establishing maritime exclusion zones
- 5.2 Extending the scope of the ISPS Code to facilities used by non-SOLAS ships (domestic & foreign)
- 5.3 Information and intelligence sharing
- 5.4 Standardizing port access and egress monitoring

10:40 – 11:00 **Break**

11:00 – 12:10 **Session 6 topics** (approx. 40 minutes per topic):
- 6.1 Community outreach & education programs
- 6.2 Extending the scope of port-wide exercises to include all relevant stakeholders, new types of threats and resumption of operations

12:10 – 12:30 **Session 7 topic** (approx. 50 minutes):
- 7.1 Security training for Designated Authority and port personnel

12:30 – 13:30 **Lunch**

13:30 – 14:00 **Session 7 continued**

14:00 – 14:45 **Session 8 – Roundtable discussion to identify good practices for**:
- strengthening port facility security oversight programs
- strengthening port security frameworks

14:45 – 15:00 **Break**

15:00 – 15:45 **Session 9 - Roundtable discussion to identify recommendations for consideration by workshop sponsors**

15:45 – 16:00 **Session 10 - Round-table assessment of workshop and next steps**

End of workshop