



Australian Government  
Department of Foreign Affairs and Trade



# APEC: Best Practice in Secure Trade



Australian Government

Department of Foreign Affairs and Trade

# APEC: Best Practice in Secure Trade



© Commonwealth of Australia 2004

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth available from the Department of Communications, Information Technology and the Arts. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Intellectual Property Branch, Department of Communications, Information Technology and the Arts, GPO Box 2154, Canberra ACT 2601 or posted at <http://www.dcita.gov.au/cca>.

Disclaimer: While every care has been taken in ensuring the accuracy of the information provided, the Department of Foreign Affairs and Trade, its officers, employees and agents, accept no liability for any loss, damage or expense arising out of, or in connection with, any reliance on any omissions or inaccuracies in the material contained in this publication.

ISBN 0-9751486-2-1

APEC Branch  
Department of Foreign Affairs and Trade  
R G Casey Building  
John McEwen Crescent, Barton  
Canberra ACT Australia 0221

Telephone: (+61) 2 6261 1111  
Facsimile: (+61) 2 6261 3009  
Email: [apec@dfat.gov.au](mailto:apec@dfat.gov.au)  
Internet: <http://www.dfat.gov.au>

Design, typesetting and printing by National Capital Printing

# Acknowledgements

The Department of Foreign Affairs and Trade's APEC Branch prepared this report to highlight efforts in APEC economies to secure trade and to disseminate information on best practice and lessons learnt to assist in future efforts in this area.

The Department of Foreign Affairs and Trade wishes to thank the many people who provided information and advice for this report, particularly those providing case study information.

From the United States, we thank Lysbeth Rickerman of the National Center for APEC; Chee Kean Lim of Savi Technology; and Thomas Wilson and Greg Hafer of BearingPoint, Inc.

From Chile, we thank Vice Admiral Codina and Lt. Commander Mrugalski of the Chilean Navy; Commander Marcelo Albarrán, Head of Information Technology Department, and Viviana Espinosa and Myriam Meylan, Translation Division, International Affairs Department, Directorate General of the Maritime Territory And Merchant Marine (Dirección General del Territorio Marítimo y de Marina Mercante, DIRECTEMAR); and Chilean Ambassador Mario Artaza, Executive Director of the APEC Secretariat.

From Malaysia, we thank Karthik K, Technical Director, Inventor, Multimedia Glory Sdn. Bhd.; Lalitha Kaleedhass, Managing Director, Inventor, Multimedia Glory Sdn. Bhd.; N. Srikanthan, Executive Director, Inventor, Multimedia Glory Sdn. Bhd.; Mohd Fauzi Abdul Hamid, Manager, Malaysia Airports Technologies Sdn. Bhd.; and Dato' Abd. Hamid Mohd Ali, Senior General Manager, Malaysia Airports Berhad.

From Australia, we thank Phil Thurbon and Simon De Vere of the International Border Initiatives Section, Entry Policy and Systems Branch, Department of Immigration and Multicultural and Indigenous Affairs; Ric Power, Deputy Director, Money Laundering Targeting, AUSTRAC; and David Hickman, Director, E-Security Policy, Information Economy Division and Gabrielle Crick, Department of Communications, Information Technology and the Arts.

From Indonesia, we thank Dr I Gde Made Sadguna, Deputy Head, Financial Transaction Reports and Analysis Centre (Pusat Pelaporan dan Analisis Transaksi Keuangan, PPATK); Deeny Uli Rosa, International Workstream and Legal Workstream, PPATK and Djoko Kurnijanto, PPATK; James Agee, Chief of Party, ELIPS II (Economic Law, Institutional and Professional Strengthening Project), Law Faculty Post-Graduate Program, University of Indonesia; Dharmawan Ronodipuro and Eddy Mulya, Counter-Terrorism Coordinating Desk (Desk Koordinasi Pemberantasan Terorisme, DKPT), Coordinating Ministry for Politics and Security.

From the APEC Secretariat and related working groups, we thank Bruce Bennett, Director (Program), New Economy–e-APEC Task Force; Sergey Shipilov, Director (Program), Transportation Working Group; and Charles C. José, Director (Program), Finance Ministers' Process.

From the Organisation for Economic Co-operation and Development, we thank Barrie Stevens, Deputy to the Director, Forum for the Future Conferences, Advisory Unit

on Multi-Disciplinary Issues, General Secretariat; William Nicol, Head of Division, Policy Coherence, Development Co-operation Directorate; Danny Scorpecci, Principal Administrator (Maritime Transport, Shipbuilding), Transport Division, Directorate of Science, Technology and Industry; Anne Carblanc, Principal Administrator (Information security and privacy, Consumer Policy) and Sven Moers, Administrator (Information security and privacy, Consumer policy), Information, Computer and Communications Policy Division, Directorate of Science, Technology and Industry; Jack Short, Secretary-General, European Conference of Ministers of Transport; and Anthony Kleitz, Head of Division, Trade Liberalisation and Review, Trade Directorate.

At Australian overseas missions, we thank Ben Clanchy, Third Secretary (Economic), Jakarta; Catherine Yates, First Secretary (Development Cooperation), Australian Agency for International Development, Jakarta; Jo Lumb, Second Secretary (Political/Economic), Santiago de Chile; and Monica Gomez, Interpreter/Research Officer, Santiago de Chile.

# TABLE OF CONTENTS

<b>Acknowledgements</b>	<b>iii</b>
<b>Executive Summary</b>	<b>3</b>
<b>Chapter 1</b>	<b>7</b>
<b>Chapter 2</b>	<b>13</b>
<b>Chapter 3</b>	<b>27</b>
<b>Chapter 4</b>	<b>39</b>
<b>Appendix – Case Studies</b>	<b>43</b>





# Executive Summary

This report highlights the active role APEC has played in addressing counter terrorism issues, particularly as they impact upon regional and global trade. It examines the experiences of individual APEC economies in securing their trade, with a view to identifying best practices that may assist others in the design and development of their responses. In many cases significant trade facilitation benefits have accrued from the application of counter terrorism measures.

## APEC, Counter Terrorism & Secure Trade

Economic integration is crucial to the future growth and prosperity of the region. APEC, which represents over 60 per cent of global GDP, has worked to liberalise trade and promote a global trading system which is open, fair and transparent. At the same time there is a realisation in APEC that acts of terrorism in the region have a potentially serious impact on regional trade, investment and people flows. The threat of terrorism to APEC economies is a shared one, making collective action the most appropriate response.

APEC Leaders first made a statement condemning acts of terrorism in 2001. In 2002 they agreed to work together to secure the flows of goods and people through a Secure Trade in the Region (STAR) initiative. The STAR initiative includes efforts to protect cargo, ships engaged in international voyages, international aviation, and people in transit; halt terrorist financing; and promote cyber security. In 2003, Leaders dedicated APEC not only to advancing the prosperity of economies, but also to the complementary mission of ensuring the security of their people.

This report focuses predominantly on what can be learnt from the progress of APEC's STAR agenda since its adoption in 2002, and, in particular, the experiences of individual APEC economies in implementing their commitments. STAR's success – realised and potential – as a tool for strengthening regional security and prosperity, can be attributed to APEC strengths in effective information sharing; cooperation among economies; and well targeted capacity-building activity.

## Best Practice in secure trade initiatives

This report examines five projects, drawn from a diverse range of APEC economies, which respond to the threat of terrorism under the STAR initiative. Based on the case studies, some common features of successful projects that aim to secure trade are:

- an ability to demonstrate benefits, both in terms of improved security and efficiency, to stakeholders and users;
- evidence of strong planning in each stage of project cycle;
- flexibility and built-in capacity for change at a minimal cost;
- strong stakeholder interaction, including between the public and private sectors;
- where relevant, the effective use of available and new technology;
- strong education and capacity building components;
- capacity to expand system or framework to other economies/interoperability; and
- international cooperation, where appropriate.

A comprehensive list of best practices appears in Chapter 4.

Case studies, further detailed in the Appendix, all necessarily involve secure trade outcomes. They demonstrate some or many elements of best practice outlined in this report. Most case studies have been able to demonstrate that secure trade actions can generate significant efficiency gains, which have the potential to exceed the cost. A brief summary of key findings follows:

#### **US/Thailand's STAR-Bangkok/Laem Chabang Efficient and Secure Trade (BEST) Project – Container cargo security**

- The BEST project aims to strengthen end-to-end supply-chain security and lower the probability of a terrorist attack utilising shipping containers through the use of advanced technology to track cargo. It also aims to facilitate international trade, enhance Thai trade competitiveness, increase business confidence in trans-Pacific trade lanes and strengthen US-Thai economic relations.
- Effective implementation of BEST has required close consultation between the Thai and US Governments and the public and private sectors; and demonstration of its benefits to business.
- Trade benefits resulting from BEST include:
  - greater overall efficiency
  - improved in-stock rates
  - lower bill of lading surcharges
  - improved container tracking
  - reduced stock requirements
  - fewer theft incidents
  - reduced insurance and problem resolution costs
  - improved customer service

#### **Chile's Graficación Marítima (GRAFIMAR) – Geographical information system for maritime security**

- The GRAFIMAR system enhances the capacity of the Chilean Navy to improve security through technology, which allows the position of a ship at sea to be tracked – on a real time basis.
- The Chilean Navy has undertaken to make this technology available to other regional users as desired, broadening its benefits regionally.
- GRAFIMAR has improved the timeliness and ease with which ships can be traced by the Chilean Navy, which leads to not only security benefits but also resource efficiencies.

#### **Malaysia's Karsof™ Total Airport Security System at KLIA – Biometric airport security**

- The Karsof™ Total Airport Security System builds on existing technology to establish a secure environment in the Kuala Lumpur International Airport (KLIA) through the use of biometrics to identify authorised visitors.
- Implementation of the system has required substantial planning, education of airport staff, and review and modification at each stage of project implementation.
- The use of 'best practice' principles have led to greater efficiencies than what would have otherwise been evident in terms of the ease with which staff and passenger movements can be monitored; and the interoperability of the system with other databases.



### **Australia's Advance Passenger Processing (APP) – Business mobility and human security system**

- The Advance Passenger Processing (APP) system improves security and facilitates people movement by providing government border agencies with advance notice of a passenger's arrival on a particular flight or vessel. It ensures that persons who are not authorised to enter are prevented from boarding vessels bound for Australia.
- The implementation of this technology involved collaboration with border control and other relevant agencies. As the system has been made available for adoption by other APEC economies on a voluntary basis, the project also has a strong capacity-building element.
- Planning and development of the APP system, from the outset, involved the twin goals of security and efficiency. Efficiencies realised in implementation of the system include:
  - unparalleled level of service delivery to passengers, airlines, airport operators and taxpayers through reduced passenger processing times;
  - flexible procedures and methods for data collection; and
  - the opportunity to minimise costs through cooperation, communication and consultation between airlines and government, as well as through utilising existing networks and systems.

### **Indonesia's Anti-Money Laundering (AML) & Anti-Terrorist Financing (ATF) Regime – Regime to combat terrorist financing**

- Indonesia's AML/ATF regime aims to prevent terrorist financing by criminalising it; and enhances Indonesia's capacity to implement criminal law and regulation, and to cooperate in financial exchange with overseas agencies.
- The regime is a strong example of cooperation domestically with financial institutions and their regulators, law enforcement agencies, the judicial sector and the government; and internationally with donor agencies, to achieve overall aims.
- Wider potential economic benefits of Indonesia's AML/ATF regime relate to increased confidence in Indonesia's financial system, both domestically and internationally, and a possible decrease in crimes relating to money-laundering, such as narcotics and corruption crimes.



# Chapter 1

*As we accelerate our progress against terrorism, APEC economies must also move to meet the challenge of encouraging global economic growth and bringing the benefits of global markets to all our peoples. Consequently, we must grow our economies even as we protect our borders and find new ways to secure our key economic infrastructure from terrorist attacks.*

*APEC Leaders' Statement on Fighting Terrorism and Promoting Growth  
26 October 2002*

## Introduction

Terrorism is a threat to economic stability, regional peace and security, a direct challenge to the Asia-Pacific Economic Cooperation (APEC) vision of free, open and prosperous trade and an affront to the fundamental values that APEC member economies share.<sup>1</sup> Thus, one of APEC's major aims is to protect the regional community from the threat of terrorism. At the same time, APEC aims to ensure that the need to combat terrorist threats does not obstruct trade (APEC, 2004).

This report aims to derive best practices from secure trade measures taken in APEC economies through their Secure Trade in the APEC Region (STAR) initiatives so that the design and development of future projects might be improved. The focus of the report is on best practices which will have future applicability rather than on the detail of the projects themselves (note that the STAR initiative is still quite new and some projects are ongoing, making case studies useful tools rather than an appropriate focus of the report). Most involve implementation of new technology aimed at making trade more secure, while at the same time increasing efficiency. The report describes experiences with the various projects, highlighting successes and identifying areas where difficulties were encountered and the strategies used to overcome those difficulties. The report also recommends strategies by which economies can find the balance between the costs and benefits of implementing secure trade.

## Costs of Terrorism and Benefits of Working Together

Increasing global integration means that opportunities for terrorist activity have expanded. It also means that the costs of terrorism are borne not only by the economy under attack, but impact more widely upon regional and global prosperity. It is therefore necessary for economies to work together to implement counter terrorism measures and minimise the cost of terrorism to the region and the world.

An economy can suffer very high costs as the result of a well-placed terrorist strike. These costs include the immediate costs of damage, loss of life and a fall in short term economic activity. Longer term costs also exist as continuing uncertainty regarding the security environment of the economy reduces confidence in the business and investment environment of the economy and increases risk perceptions and risk premiums. This, in turn, can lead to a reduction in investment and economic growth. Estimates of such costs are documented in various studies (for a fuller discussion of the various costs, see Economic Analytical Unit, 2003 and 2004). For example:

<sup>1</sup> APEC's 21 member economies are Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; Philippines; Russia; Singapore; Chinese Taipei; Thailand; United States and Viet Nam. The word 'economies' is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities ([www.apec.org/apec/member\\_economies.html](http://www.apec.org/apec/member_economies.html), accessed 5 August 2004).



- the International Monetary Fund estimated that the cost to the US economy of the September 11 2001 terrorist attacks was around 0.75 per cent of gross domestic product (GDP) per year;
- the US Congressional Budget Office estimated that terrorism directly cost the United States about 0.3 per cent of GDP in the non-farm business sector in 2002 and reduced total factor productivity by roughly 0.3 per cent for 2002 and later years;
- the Bureau of Labour Statistics estimated that the attack on the World Trade Center cost New York City 430 000 lost job months and wage losses of US\$2.8 billion with effects greatest in the high paid 'export' economy of banking, finance and insurance (International Monetary Fund, 2001, Congressional Budget Office, 2002 and Dolfman and Wasser, 2004);
- a study of over 200 countries from 1968 to 1979 found that a doubling in the number of terrorist incidents decreased bilateral trade by about 6 per cent and that between 1975 and 1991, heightened terrorist activity reduced average annual net FDI inflows to Spain and Greece by 13.5 and 11.9 per cent respectively (Nitsch and Schumacher, 2002 and Enders and Sandler, 1996).

However, the costs of terrorism are not limited to the economy targeted by an attack; due to regional and international economic linkages, terrorist events in one economy can impose significant costs on other economies as well. The costs of terrorism are likely to be even higher for developing economies, as they have a greater reliance on trade and capital flows. The costs to other economies flow through trade networks. For example:

- analysts estimated that the two week lockout at 29 US West Coast ports in late 2002 cost Asian economies around 0.4 per cent of nominal GDP (Saywell, 2002);
- modelling of a 0.5 per cent decline in primary factor productivity due to terrorism showed that over the following five years *world* economic activity would be around 0.7 per cent (or around US\$310 billion in 2003 dollars) lower than would otherwise be the case; simulations a of rise in risk primarily due to terrorism show that the adverse economic impact of terrorism stemming from increased risk perceptions could be greater than those emanating from declining productivity (Economic Analytical Unit, 2004);<sup>2</sup>
- the same modelling also suggests that developing economies suffer more significant declines in economic growth (in relative terms) from terrorism than developed economies as the results indicate that ASEAN's economic activity would be around 1.4 per cent lower than the reference case by 2008, compared to the worldwide impact of 0.7 per cent lower than baseline (Economic Analytical Unit, 2004).

Combating terrorism does involve upfront costs. However, the costs of counter terrorism measures should be viewed as an investment that will reduce risk premia and the bias uncertainty creates against longer term, productivity-raising activities. The costs can also be shared between economies if they cooperate on counter terrorism issues. Furthermore,

2 Terrorism reduces productivity and hence GDP as resources are diverted from more productive activities to higher security spending. Worldwide reappraisal of equity risk causes investors to redistribute funds, moving out of stocks and other riskier high return investments into more secure investments such as bonds, causing worldwide investment and thus GDP to fall.



there is evidence that the costs of implementing counter terrorism measures are less than the potential cost of a major terrorist attack (OECD, 2003). Implementing these measures collectively can also result in shared economic efficiencies over the longer term and a more secure regional and global investment environment.

### **Counter Terrorism Measures for Trade Efficiency and STAR Initiative**

Due to the high costs of terrorism and the benefits of cooperation, APEC actively supports economies in their efforts to introduce counter terrorism and secure trade measures (see Chapter 2 for APEC activities).

In approaching secure trade, APEC is conscious that the introduction of perfect security could impose onerous costs – dramatically reducing productivity and prosperity. Creating the right balance between competitiveness and security is therefore a critical challenge. There is no security without economic vitality, just as there is no economic vitality without a secure environment in which to live, work, produce and trade (Council on Competitiveness, 2004).

While globalisation creates growth opportunities, it also adds complexity to supply chain management, partly due to increasing demands from security. Traditional approaches to security involving defences such as guards and gates are a productivity drain rather than a productivity enabler. There is a risk that overly prescriptive security standards could unduly reduce productivity and dampen growth prospects. Another dilemma that arises when introducing counter terrorism measures is that the critical infrastructure and assets that require protection are diverse, with many being privately owned and controlled.

The means exist to overcome these problems. Innovative approaches can embed security efficiently across existing operations to protect competitiveness and thus achieve net benefits (Rosencrance, 2003). New technologies, along with new management processes, risk management tools and workforce training have the potential to facilitate trade by simultaneously achieving higher security and productivity (see next section for more details on such new technologies). In this way, trade security is not merely a way to prevent terrorism but is also an opportunity to simplify and streamline supply chain processes. The case studies examined later in this paper are good examples of such innovative approaches to facilitating secure trade.

Also important in enhancing security measures, while facilitating trade, is cooperation between APEC's 21 economies – particularly in terms of introducing new procedures and implementing internationally accepted standards (APEC, 2004). Cooperation, along with new technology and processes, will keep costs down and can result in greater efficiency within a secure global and regional trading environment. For example, returns on investment in new technology will be higher the larger the number of other users and the network effects from wider adoption reduce costs and make a system easier to operate (Pacific Economic Cooperation Council, 2004).

APEC's first major initiative aimed at achieving secure trade in the region cooperatively, while minimising costs, is the Secure Trade in the APEC Region (STAR) agenda. The STAR agenda covers a range of activities that support economies in their efforts to secure trade (by



protecting cargoes, international shipping and aviation and people in transit), to halt terrorist financing and to promote cyber security. Importantly, it also seeks to ensure free and secure trade is achieved through cooperation and capacity building.

### **New Technologies for Trade Security**

As mentioned above, there are a range of new technologies that can underpin trade security. One of them, biometrics, involves identifying and authenticating individuals based on measurable physical characteristics that can be automatically checked, such as fingerprints, facial features or iris analysis (see Malaysia's airport security system case study at Appendix A3 for experiences with implementing a biometric identification system).

Another such technology is radio frequency identification (RFID). RFID consists of two components: a tag (also called a transponder, which includes a computer chip and an antenna) and a reader (also called an interrogator). The tag contains a small amount of memory for holding data and when it comes into proximity with the reader, the reader will detect the tag's presence and read the data. The data can identify the specific object or provide information about it. The communication mechanism is radio waves at a particular frequency so there is no need for a direct 'line of sight' between the reader and the tag (OECD, 2004). This application can be used for purposes such as inventory control and supply chain and transport management. On the security side, when used with a lock, it provides a way to identify and track containers and verify their contents (see the BEST case study at Appendix A1 for details of a project using this technology).

Global satellite tracking is another technology which can be used to fight terrorism. Global satellite navigation involves satellites orbiting around the earth in a number of orbital planes emitting signals. Signals from at least four satellites are required to determine the position of a receiver on the earth's surface. Applications for satellite navigation include tracking and control for the transport of hazardous goods; onboard navigation for maritime transport; fleet management for various transport modes; continuous monitoring of structures in civil engineering; environmental and geophysical monitoring; personal navigation and protection; disaster monitoring; and law enforcement. On the security side, authorities can utilise this technology to track suspect shipping (see Appendix A2 for information on Chile's geographical information system).

Developing and implementing these new technologies and processes can impose costs, both planned and unplanned. Examining case studies of APEC economies' experiences with these technologies and processes provides lessons on the best ways to introduce them and the pitfalls to avoid. It also allows the identification of best practice.

### **What is Best Practice?**

'Best practice' is a guide for how to best perform or implement an activity. It is usually identified through reviewing performance indicators and assessing outcomes of activities already undertaken. Once identified, best practice is used to improve the performance of other comparable activities.



## Box 1 Some Definitions of Best Practice and Benchmarking

### Best Practice

The winning strategies, approaches, and processes that produce superior performance in an organisation. A best practice is a by-product of a successful end-result. (<http://www.portal-step.com/90.IGlossary.htm>)

The concept of best practice is not reserved only for 'ultimate truths' or 'gold standards.' ... best practice means accumulating and applying knowledge about what is working and not working in different situations and contexts. In other words, it is both the lessons learned and the continuing process of learning, feedback, reflection and analysis (what works, how and why, etc.). (<http://www.unaids.org/bestpractice/Collection/summary/introduction.html>)

An activity or procedure that has produced outstanding results in another situation and could be adapted to improve effectiveness, efficiency, ecology, and/or innovativeness in another situation. (<http://www.ichnet.org/glossary.htm>)

A superior method or innovative practice that contributes to the improved performance of an organisation, usually recognized as 'best' by other peer organisations.

A technique or methodology that, through experience and research, has proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success. ([searchVB.com](http://searchVB.com))

### Benchmarking

A benchmark is a measurement or standard that serves as a point of reference by which process performance is measured. [GAO] Benchmarking is a structured approach for identifying the best practices from industry and government, and comparing and adapting them to the organisation's operations. Such an approach is aimed at identifying more efficient and effective processes for achieving intended results, and suggesting ambitious goals for program output, product/service quality, and process improvement. (Government Accounting Office)

An improvement process in which a company measures its performance against that of best in class companies, determines how those companies achieved their performance levels and uses the information to improve its own performance. The subjects that can be benchmarked include strategies, operations, processes and procedures. ([www.asq.org/info/glossary/b.html](http://www.asq.org/info/glossary/b.html))

Best practice in counter terrorism and trade security measures will have application in the private sector (covering businesses across the supply chain spectrum), government (including quasi-public agencies such as port authorities) and for other stakeholders (such as travellers). Key issues for trade security, to be reflected in best practices, include:

- identification of critical assets and supply chain weaknesses, the threats to them and their vulnerabilities;
- assessment of technologies' ability to achieve security while facilitating trade, and the ease of their interface with other systems;
- strategic planning and evaluation of measures put in place;
- effective training and learning of practices and procedures to ensure that there is sufficient expertise available, whether in-house or outsourced;
- constructive relationships between the private and public sectors;
- sustained support of governments and stakeholders;
- a focus on outcomes; and
- as appropriate, reliance on local partners and international cooperation.

These are discussed further in Chapter 3.

### **Purpose of this Report**

This report aims to assist policymakers and other stakeholders (private and public sector) develop and implement innovative solutions to trade security problems posed by the increased threat of terrorism. Through analysis of case studies on various trade security measures, this report identifies best practice principles which can be used to:

- raise awareness of the issues and practices surrounding improved security;
- share and transfer knowledge, expertise and experience;
- design and implement new trade security projects or to make current programs more effective;
- receive timely, comprehensive information about other economies' security efforts so that they are better prepared to react to emerging issues; and
- improve outcomes on trade security by learning about what works and what is less effective from the examples of other APEC economies grappling with similar issues.



## Chapter 2

### APEC's Counter Terrorism Agenda and STAR Developments

#### Why APEC Has a Secure Trade Agenda

APEC's 21 member economies represent one third of the world's population, about 60 per cent of world gross domestic product and around half of world trade (APEC, 2004). The APEC region is also home to several significant financial and banking centres, such as Hong Kong and Singapore. It is therefore likely that the global economy would feel the flow-on effects of any terrorist acts in the region.

APEC's trade has generally grown faster than world trade, however foreign direct investment (FDI) has fallen in many economies. Between 1990 and 2003, APEC's merchandise exports grew by an annual average of 7.3 per cent, compared to growth in world merchandise exports of 6.1 per cent (World Trade Organization, 2004). Intra-APEC trade grew even faster: between 1990 and 2002, intra-APEC merchandise exports grew by an average of 7 per cent each year, compared with 4.8 per cent for extra-APEC merchandise exports (World Trade Organization, 2004).<sup>3</sup>

APEC's importance in world trade is reflected in trade infrastructure in the region. For example:

- APEC economies host 21 of the world's 30 top seaports and 23 of the world's 30 busiest airports (Juster, 2003).
- In maritime trade, in 2001, the eight largest Asian ports handled 60.8 million (United Nations Conference on Trade and Development, 2003b) – over one quarter of all movement in cargo containers between major seaports.
- Over 43 per cent of containers entering the United States annually arrive from 11 Asian megaports.
- Much maritime cargo traffic goes through the Malacca and Singapore Straits, which are vulnerable to attack and piracy; impediments to traffic through these straits would disrupt world commerce, bearing in mind that 80 per cent of the oil imported by East Asia travels through these waters.

Tourism is also an important link between the economies of the APEC region and those of the rest of the world. Tourism is already the largest employer in the Asia-Pacific region; it provides substantial income and employment, and it also stimulates regional economic growth. Air travel is set to expand in Asia, with strong growth in international visitors and several lower cost airlines starting operations. In 2002, APEC's share of international tourist arrivals was around 30 per cent, largely unchanged from 1995, due to post-2001 declines in North America. However, between 1995 and 2002, tourism to North-East and South-East Asia grew strongly by an annual average of 6.4 per cent (World Tourism Organization, 2003). Even after the impact of SARS in 2003, destinations in Asia show a strong rebound with most Asian destinations growing by over 15 per cent in the year to the end of April 2004 (World Tourism Organisation, 2004).

<sup>3</sup> Many developed countries experienced a sizeable decline in FDI inflows influenced by continuing weak economic conditions. A large part of the decline in the United States was due to repayments of loans by foreign affiliates to parent companies, presumably to take advantage of the lower interest rates in the United States, and for other reasons, such as improving parent firms' debt-to-equity ratios. Notably, cross-border mergers and acquisitions plunged (United Nations Conference on Trade and Development, 2003a).



Maintaining and protecting the trade infrastructure while maintaining commercial ties/flows in the APEC region is therefore not only critical to APEC economies, but also to the rest of the globe that uses and relies on this infrastructure. APEC Leaders agreed, therefore, at their annual meeting in Los Cabos, Mexico, October 2002, to work together to secure the flow of goods and services in the region. To do this, trade channels need to be kept clear while the security surrounding the world's transportation infrastructure is strengthened, and sectors supporting trade and commercial ties, notably the information technology and financial sectors, need to be protected and strengthened to counter terrorist threats.

### APEC's Security and Counter Terrorism Activities

Since making its first statement on counter terrorism in 2001, APEC has implemented and continues to develop a strong program of activities to assist member economies deal with countering potential terrorist threats (Table 1). In the years since, APEC has also taken steps to speed up the implementation of commitments, to monitor their progress and to build the capacity of member economies to respond to the threat of terrorism (APEC, 2004).

**Table 1 Summary of Main APEC Counter Terrorism Activities**

Date	Initiative	Action
October 2001	APEC Leaders Statement on Counter-Terrorism, Shanghai, China	Reaffirmed importance of forging ahead to achieve Bogor's goal of free, open trade and investment Committed to collective actions to support the global fight against terrorism.
September 2002	APEC Action Plan on Combating the Financing of Terrorism	Finance Ministers endorsed a comprehensive approach to preventing the funding of terrorism, including improved international cooperation and a greater focus on means of financing terrorism outside of the mainstream financial system.
October 2002	APEC Leaders 2002 Statement on Fighting Terrorism and Promoting Growth, Los Cabos, Mexico	Committed member economies to further measures to combat terrorism and to a specific timetable for their adoption in three areas: securing the movement of goods and people, halting financial flows to terrorists and promoting cyber security. A key element is the Secure Trade in the APEC Region (STAR) initiative.
February 2003	APEC Senior Officials established the Counter Terrorism Task Force (CTTF)	Coordinated the implementation of the Leaders' Statement on Fighting Terrorism and Promoting Growth. Met in the margins of the APEC Senior Officials' Meetings and also held informal talks.
February 2003	APEC Senior Officials Counter Terrorism Action Plan	Facilitated the implementation of the measures contained in the Leaders' 2002 Statement.



February 2003	First Secure Trade in the APEC Region (STAR) Conference, Bangkok, Thailand	Key players from a broad range of official agencies and leading companies brought together. The conference highlighted a range of programs to facilitate the secure movement of goods and people in the APEC region.
August 2003	APEC Counter-Terrorism Action Plans (CTAP)	CTTF initiated development of concise summaries of measures being undertaken by economies to implement the 2002 APEC Leaders' Statement, along with related capacity building needs of economies.
September 2003	High-Level Meeting in Maritime Security Cooperation, Manila, The Philippines	Meeting devised an APEC-wide framework of exchange information on maritime security, to identify capacity building needs to implement the International Maritime Organization's (IMO) ISPS and SOLAS maritime security requirements and to strengthen cooperation with the private sector.
March 2004	Second STAR Conference, Viña del Mar, Chile	A key theme was public-private sector collaboration. The conference covered maritime security, air transportation security, the mobility of people and measures to prevent terrorist financing.

Source: APEC, various years, [www.apec.org](http://www.apec.org).

## 2002 APEC Leaders' Statement and the STAR Initiative

In Los Cabos in October 2002, APEC Leaders agreed to a comprehensive *Statement on Fighting Terrorism and Promoting Growth*. This statement gave rise to Secure Trade in the Region (STAR) initiative. The goal of STAR is to:

- ensure the security of trade and travel while improving the efficient flow of goods and travellers;
- halt terrorist financing (in line with the APEC Action Plan on Combating the Financing of Terrorism that aims to deny terrorist access to the world's financial system);
- promote cyber security (in line with the APEC Cyber security Strategy to protect communications and information systems); and
- enhance cooperation, new procedures and greater use of advanced technology to ensure success.

APEC's STAR initiative is a strong program of secure trade activities, which aim to strengthen security against terrorist threats while simultaneously boosting trade efficiency. This includes in the areas of: (a) aviation security; (b) maritime security (e.g. measures to protect cargo, ships engaged in international voyages, and ports); (c) business mobility and human security (e.g. measures related to immigration processes to enhance security and flows of people); (d) combating terrorist financing; and (e) cyber security. To maximise the outcomes of the STAR initiative, APEC economies have also committed to monitoring the implementation of initiatives in the above areas, as well as to providing and undertaking capacity building activities where necessary.

### *Protecting Cargoes*

APEC members agreed to protect cargoes by expeditiously implementing a container security regime that would assure in-transit integrity of containers, identify and examine high-risk containers and, working within international organisations, require the provision of advance electronic information on container content to customs, port, and shipping officials as early as possible in the supply chain, while taking into consideration the facilitation of legitimate trade. APEC also aims to implement the common standards for electronic customs reporting developed by the WCO that provide data to target high-risk shipments and facilitate trade, wherever possible by 2005. Promoting private-sector adoption of high standards of supply chain security, as developed by the private sector and law enforcement officials, is also planned.

### *Protecting Ships Engaged in International Voyages*

APEC aims to protect ships engaged in international voyages. Members agreed to promote ship and port security plans by July 2004, i.e. by providing assistance where necessary in complying with the International Ship and Port Facility Security (ISPS) Code, and by installing automatic identification systems on certain ships by December 2004.<sup>4</sup> Members also agreed to enhance cooperation between APEC fora and organisations such as the International Maritime Organization (IMO) and the International Maritime Bureau Piracy Reporting Center and to fight piracy in the region.

### *Protecting International Aviation*

Member economies agreed to protect international aviation by improving airline passenger and crew safety through introducing highly effective baggage screening procedures and equipment in all APEC international airports as soon as possible and, in any case, by 2005. They also agreed to implement standards for reinforced flight deck doors for passenger aircraft more quickly, by April 2003 wherever possible. Further, they agreed to support International Civil Aviation Organization (ICAO) mandatory aviation security audits through the *Support for Aviation Security Audits Phase I: Preparation for ICAO Universal Security Program Audits* project, which is helping developing APEC economies prepare through specialised training. Members also agreed to enhance air cargo security by promoting adoption of the guidelines developed by ICAO and the International Air Transport Association (IATA).

### *Protecting People in Transit*

Member economies agreed to protect people in transit by implementing as expeditiously as possible a common global standard based on UN EDIFACT for the collection and transmission of advance passenger information, by adopting standards for application of biometrics in entry and (where applicable) exit procedures and

---

<sup>4</sup> Agreed to in December 2002, the ISPS Code, which forms part of the International Convention for Safety of Life at Sea (SOLAS), is a comprehensive set of measures to enhance the security of ships and port facilities. Its approach is that ensuring the security of ships and port facilities is a risk management activity requiring an assessment of the risks in each particular case to determine appropriate security measures. It provides a standardised, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities. It contains detailed security-related requirements for governments, port authorities and shipping companies along with a series of guidelines about how to meet these requirements ([www.imo.org](http://www.imo.org), accessed 5 August 2004).



travel documents, such as those being developed by the ICAO and the International Standards Organization, and by ensuring the highest possible integrity of all government officials who are involved in border operations (APEC, 2002).

### *Halting Terrorist Financing*

APEC economies agreed to work together to deny terrorists access to the world's financial system and use the money trail to locate and apprehend terrorists. Members agreed to fully implement related UN and other international instruments. They were to endeavour to ratify the International Convention for the Suppression of the Financing of Terrorism no later than October 2003. They also agreed to support the Financial Action Task Force's (FATF) Eight Special Recommendations on terrorist financing and pledged to comply as quickly as possible with them. As such, APEC economies called on the IMF and World Bank, in coordination with the FATF, to begin conducting integrated and comprehensive assessments of countries' efforts to implement these recommendations, and identified jurisdictions which needed technical assistance.<sup>5</sup> APEC members also committed to implementing quickly and decisively all measures needed to prevent terrorists and their supporters from accessing the international financial system, as called for in UN Security Council Resolutions 1373 and 1390, which include:

- effective blocking of terrorist assets;
- criminalisation of the financing of terrorism;
- increased efforts to investigate and prosecute money launderers and terrorist financiers;
- preventive steps to protect the integrity of the financial system by regulating and supervising the financial sector consistent with international standards; and
- joint identification and designation of targets of regional interest.

Also in an effort to halt terrorist financing, member economies agreed to promote better monitoring of alternative remittance systems and non-profit organisations by supporting the work of APEC finance officials and regional bodies on alternative remittance systems, including an analysis of the factors that encourage their use. They further agreed to protect non-profit organisations and well-meaning donors from having their funds misused by terrorist financiers and endorsed FATF's recently announced best practices for preventing abuse of charitable institutions by terrorists.

Member economies also undertook to enhance law enforcement and regulatory capabilities by establishing or identifying by October 2003 their own financial intelligence unit (FIU) and taking steps to enhance information sharing with other FIUs. They were also to support private sector initiatives aiming at monitoring the finance services industry,

---

<sup>5</sup> The FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. It monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. Its membership is currently made up of 31 countries and territories, and two regional organisations ([www.fatf-gafi.org](http://www.fatf-gafi.org), accessed 9 July 2004).

such as the Wolfsberg Statement on the Suppression of the Financing of Terrorism, and endorse cooperation between financial institutions and governments.<sup>6</sup>

### *Promoting Cyber Security*

The Leaders' Statement also seeks to protect the global communications network that supports international trade and commerce. APEC economies collectively committed to endeavour to enact a comprehensive set of laws relating to cyber security and cyber crime consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001), by October 2003. They also agreed to identify national cyber crime units and international high technology assistance points of contact, where such capabilities did not already exist by October 2003, and establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003. The statement also called for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime.

### *Implementation and Capacity Building*

To ensure success in achieving the vision of efficient and secure trade, enhanced cooperation, new procedures and greater use of advanced technology are required. APEC officials were charged with monitoring the progress of implementation.

To build on the considerable counter terrorism-related training and other assistance already being undertaken in the region, APEC has collectively committed to:

- welcome new commitments by APEC members to contribute further to these capacity building efforts;
- commend current efforts by the international financial institutions to build counter terrorism capacity in APEC economies and call on them to work with APEC members to further improve APEC member capacity;
- encourage the private sector to work in partnership with APEC economies to implement secure trade measures; and
- emphasise that counter terrorism capacity building in APEC needs to be demand driven.

Recently APEC also initiated the establishment of a Cooperation Fund for Regional Trade and Financial Security Initiative (FRTFESI), which is to be administered by the Asian Development Bank (ADB) and used to help support regional projects strengthening transportation and/or financial security. At the time of its establishment in 2004, 3 donors – Australia, Japan and the USA – were contributing approximately USD 7 million (including both cash and in-kind contributions) to the FRTFESI.

### **STAR's Achievements and Ongoing Work Program**

The STAR initiative has achieved much in a short period, including the hosting of annual STAR conferences to share and develop ideas, other high level meetings and

---

<sup>6</sup> The Wolfsberg Group, which came together in 2000 at the Château Wolfsberg in Switzerland, is an association of twelve global banks, which aims to develop financial services industry standards and related products for know your customer, anti-money laundering and counter terrorist financing policies ([www.wolfsberg-principles.com](http://www.wolfsberg-principles.com), accessed 5 August 2004).



workshops, as well as targeted activities and cooperation to achieve security goals. STAR Conferences provide an opportunity for APEC economies to share best practice solutions for solving common problems and to promote active partnerships between governments and the private sector to implement these measures.

### *STAR Conferences*

The first STAR Conference in Bangkok in February 2003, co-hosted by the United States and Thailand, brought together representatives from all APEC members, senior executives from major private sector companies, and officials from international organisations such as the IMO, IATA, WCO and the World Bank to discuss how to advance trade efficiency and trade security in the Asia-Pacific region. Participants agreed that investment in security can deliver significant economic returns, not only by reducing the economic costs of terrorism, but also by facilitating the movement of goods and people. Capacity building, in particular the need to strengthen the institutional capacity of governments, was seen as essential to STAR's success. As a follow-up to the STAR initiative, Thailand and the United States developed a pilot demonstration project, the STAR-Bangkok/Laem Chabang Efficient and Secure Trade (BEST) project (see case study at Appendix A1 for more details).

The STAR II conference in Chile in March 2004 included topics on maritime security, air transportation security, the mobility of people and measures to prevent terrorist financing. At the conference, APEC economies agreed that implementing new security measures and securing a more stable economic environment requires collaboration between the public and private sectors and a sharing of information between governments. However, there were concerns about the impact that security measures could have on trade facilitation. They agreed that a global approach towards the full implementation of the measures is vital and that it is in every economy's own interest to see that their neighbours and trading partners also proceed to meet the requirements. A high priority was also placed on international technical cooperation and the involvement of international financial institutions. Recommendations from STAR conferences are presented to APEC Officials, Ministers and Leaders for consideration and policy development.

### *Maritime Security*

In September 2003, the APEC High Level Meeting on Maritime Security agreed to:

- devise an APEC-wide framework/mechanism to enable an exchange of information on maritime security;
- draw up an indicative list of capacity-building needs of APEC economies related to the implementation of maritime security measures and present this to international financial institutions;
- prepare a list of technology requirements for a secure maritime environment for each APEC economy; and
- strengthen the cooperative partnership with the private sector to enhance maritime trade and security in the APEC region.

In particular, to safeguard the large maritime trade flows, the STAR initiative has been helping economies adopt the IMO's ISPS Codes by July 2004.<sup>7</sup> The STAR II Conference agreed that it was imperative that all economies have the appropriate laws and regulations in place to fulfil ISPS commitments, noting that failure to do so would lead to a reduction in the level of maritime trade, the closure of port facilities and a decrease in port-related business operations for economies failing to introduce new rules in the near future (APEC, 2004c).<sup>8</sup> To achieve this important task of ensuring that ships are able to load or unload cargo at APEC ports whilst meeting the new security standards, the Transportation Working Group (TPT-WG) established a special task force to help economies implement the security codes and the United States developed a website to act as a resource for APEC economies to view international efforts to implement the ISPS Code.<sup>9</sup> To assist further with applying the ISPS Code, the Transportation Working Group held a three day ISPS Code Implementation Agenda at the 23rd APEC Transportation Working Group meeting in April 2004. Detailed information was provided on how to implement legislation, conduct vulnerability self-assessments, and review and approve security plans. The APEC Transportation Working Group is also supporting the development and use of Intelligent Transportation Systems (ITS) to enhance supply chain security and increase the efficiency of trade.

The 4th APEC Transportation Ministerial Meeting in July 2004 considered further ways and means of reducing impediments to trade and investment, while enhancing security and safety (APEC, 2004a). Ministers agreed to implement an internodal supply chain security initiative over the next two years, implement arrangements for the structured exchange of information among member economies on safety and security best practices and measures, and enhance APEC's cooperation with the World Bank and the Asian Development Bank to improve transport professionals' capabilities, including in the area of international security commitments (APEC, 2004a).

Several individual economies are extending maritime security assistance to other APEC members on a one-to-one basis. These efforts will be enhanced by the recent establishment of the ADB Cooperation Fund for Regional Trade and Financial Security Initiative (FRTFESI), which will concentrate on maritime security as one of its three focus areas (the other two are aviation security and combating terrorist financing). Examples include:

- Australian assistance already provides a significant boost to the capacity of maritime security in a number of developing economies.
- Canada is providing financial support to the IMO's Maritime Security Trust Fund to assist APEC economies to prepare themselves for international assessments and maritime security standards.

---

7 As of 30 June 2004, 53.4 per cent of all port facilities subject to the Code had Port Facility Security Plans approved and 58.6 per cent of ships liable under the Code had International Ship Security Certificates issued (International Maritime Organization, 2004).

8 After the ISPS Code's entry into force on 1 July 2004, IMO members can deny entry to ships coming from or which have transited ports that do not comply with the Code.

9 The US Coast Guard's International Port Security Program link is <http://www.uscg.mil/hq/g-m/mp/IPSP.shtml>.



- The United States also put forward a major initiative to ensure that APEC economies have the required skills and knowledge to implement and monitor compliance with the ISPS Code; it has made a group of experts available to travel to member economies that request capacity building in the area of ISPS Code implementation. At the Transportation Ministerial Meeting in July, the United States announced that it would provide US\$240 000 to fund technical and other assistance to developing economies to implement the ISPS Code.
- Japan is holding seminars on port and maritime security in both Japan and in some APEC economies to help ensure the full implementation of SOLAS/ISPS Code. Other projects are being planned.

### *Protecting Cargoes*

Under the STAR initiative, APEC customs administrations are enhancing their procedures to target high risk shipments for inspection, as well as to facilitate legitimate trade, in response to the inherent vulnerability of container transport that can be exploited by terrorists. To provide the data necessary to target these shipments, APEC economies are working to implement WCO common standards for an electronic customs reporting system. APEC is also undertaking programs, including training, to simplify and harmonise customs procedures – the Sub Committee on Customs Procedures’ work program on the Revised Kyoto Convention will help to modernise customs administration through the simplification and harmonisation of customs procedures. These improvements will improve the accuracy, certainty, uniformity and transparency of customs procedures.

Also under the STAR initiative, APEC is helping to build the systemic risk management capacity necessary to allow customs administrations to target resources where they are most needed. Other programs are helping to raise the level of integrity of customs administrations in the region and to facilitate the electronic lodgement and processing of customs-related information by importers and exporters. This will reduce or eliminate the need for paper documents in customs administration and make it easier for law enforcement personnel to target suspicious cargoes or traders. A further recommendation has also been made by the APEC Business Advisory Council (ABAC) for economies to develop an electronic single window system that covers all import and port procedures.

Sharing innovative solutions on facilitating cross border trade while increasing security has been another key aspect of the STAR initiative. For example, Canada organised an APEC symposium on the Canada-US Smart Border Agreement, and many APEC ports are participating in the United States Container Security Initiative (CSI). The CSI aims to ensure the in-transit integrity of containers and provides electronic information on a container’s contents to customs, port and shipping officials as early as possible in the supply chain. Finally, APEC members have been cooperating to strengthen border security through enhanced supply chain security guidelines. In August 2003, APEC approved its Voluntary Private Sector Supply Chain Security Guidelines. These non-binding guidelines are business friendly and are being used by the private sector to enhance their supply chain security practices.

### *Protecting Ships on International Voyages*

The STAR initiative is also helping to protect ships engaged in international voyages through capacity building programs, which assist economies adopt the ISPS Codes. Certain ships will also be assisted to install automatic identification systems by December 2004. The APEC Transportation Working Group is developing standards for detection equipment and other security technology.

Responding to the threat of piracy and terrorism in the main maritime straits of South-East Asia, APEC fora are increasingly cooperating with organisations such as the IMO and the International Maritime Bureau's Piracy Reporting Centre. The Transportation Working Group is also helping to develop a system for accrediting manning agents who provide many of the 1.2 million seafarers employed by maritime companies. Plans also are underway to develop a policy on seafarers' documentation to ensure that only bona fide seafarers are employed on vessels.

### *Protecting International Aviation*

Through the TPT-WG, the STAR initiative is involved in enhancing the safety and security of airline passengers and crew through capacity building and training programs. Programs are underway to help economies meet international safety standards and to ensure that aviation personnel are properly trained and have the necessary resources to carry out their responsibilities.

Further measures are needed to deliver a more effective approach to air transportation security in the APEC region. These could include:

- the training of personnel to monitor suspicious activities and report incidents;
- cargo security programs to ensure the legitimacy of shippers;
- air cargo data validation systems and identification of high risk cargos by means of effective canine detection services;
- enhanced risk assessment methodologies;
- the establishment of security teams to consider intelligence information collection and coordinated action, not only within aviation companies, but also within civil aviation authorities;
- improved domestic regulations, incident reporting, monitoring and continuous surveillance systems; and
- the use of air marshals to prevent international terrorism.

### *Protecting People in Transit*

APEC economies are developing standards for the implementation of Advance Passenger Information (API) systems, including applying biometrics to and improving the security of travel documentation, as well as ensuring the highest levels of integrity of all border officials.<sup>10</sup>

10 API systems maximise security for genuine travellers by sending passenger information electronically to the destination border protection agency prior to the passenger's departure from an overseas airport, enabling passenger details to be pre-processed and checked against relevant alert lists, and for law enforcement personnel to make appropriate arrangements for high risk persons on their arrival (see Appendix A4 for API case study).



The implementation of API systems across the region will provide significant benefits for all economies by maximising the security of travel and facilitating faster processing of legitimate travellers, while reducing opportunities for travel by unauthorised or improperly documented persons and persons otherwise suspected of being involved in illegal activities, such as terrorism.

API systems have been developed consistent with the recommendations found in the APEC Business Advisory Council 1997 Report to Economic Leaders. This includes recommendations that APEC expand its information sharing activities in visa processing, border entry management systems and technology to include cooperation in the identification of world best practice systems and technologies. The report also recommended that priority be given to training and technical infrastructure development (Business Mobility Group, 2004). API systems also build on the APEC Business Travel Card pre-clearance system and the successful business mobility technical training and cooperation programs.

APEC standards for implementing API systems have been agreed. As of August 2004, five economies had adopted API systems and thirteen economies had completed or had undertaken to complete feasibility studies. API systems are likely to become operational in most APEC economies over the next few years. In addition and complementary to the API technology, several biometric systems are already being used in APEC economies, such as facial recognition using computer analysis, fingerprint checking and the identification of iris features.

As new measures, such as the API systems, often require substantial resources and highly specialised skills for their implementation, capacity building and funding from major donors is needed to implement them. Therefore, API is currently run as an 'APEC Pathfinder Initiative', an approach which allows economies that are ready to initiate and implement cooperative arrangements to proceed to do so, while those that are not yet ready to participate may conduct feasibility studies, undertake capacity building activities and join at a later date.

Border security is also being strengthened through the development of an APEC Regional Movement Alert List (RMAL) which will detect persons of security concern, as well as lost, stolen and fraudulent travel documentation. APEC is further strengthening the capacity of border security agencies through a range of projects by the Informal Experts Group on Business Mobility (IEGBM) covering:

- document examination and fraud detection training;
- standards in travel document security and related issuance systems; and
- standard codes of professional conduct and service for immigration officers.

Border security is strongly linked to the health of tourism in APEC economies in particular, and APEC has recognised the need to reduce the potential impact of terrorist attacks on this industry. In December 2003, the APEC International Centre for Sustainable Tourism published a practical risk management study for governments and tourist operators, finding that protecting tourism is only possible through

cooperation across nations, between and within governments and all groups in the global tourism industry.

### *Suppressing Terrorist Financing*

Since September 11, worldwide efforts to combat money laundering and the financing of terrorism have assumed heightened importance. Money laundering and the financing of terrorism are global problems that not only threaten security, but also compromise the stability, transparency and efficiency of financial systems. At least US\$1 trillion is laundered annually using increasingly sophisticated methods of moving funds across borders. Financing of terrorism is a significant global threat that undermines economic and social prosperity and development (World Bank).

As a part of their commitment to addressing these problems, APEC economies have implemented relevant international conventions and recommendations, including the International UN Convention for the Suppression of the Financing of Terrorism. Adding strength to these efforts, the Counter Terrorism Task Force (CTTF) held a seminar to provide legal policy assistance to strengthen Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) frameworks in October 2003.

APEC has also recognised a need for all member economies to have an operational FIU to prevent terrorist financing and to enhance and facilitate cooperation among APEC economies in the area of financial security, counter terrorist financing and prevention of money laundering. APEC economies are implementing relevant international conventions and recommendations; providing FIUs with broad access to a wide variety of financial information, including bank accounts and tax information; considering imposing AML/CFT obligations on independent legal professionals; and developing comprehensive national AML/CFT strategies that articulate in detail the goals of the public and private sector as partners in AML/CFT regimes and timetables for accomplishing those goals.

### *Cyber Security*

The APEC TEL e-Security Task Group has implemented several initiatives to develop a secure network environment. To prevent the criminal misuse of information, APEC economies have enacted laws relating to cyber security, consistent with the United Nations General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The capacity of institutions to implement these laws is being strengthened by the Cybercrime Legislation and Enforcement Capacity Building Project. The project is doing very well, with the first phase funded by the United States, a conference and training seminar on cyber crime laws in Thailand in July 2003. The second phase of the project (funded by APEC) was delayed due to the development of follow-on assistance. This part of the project has commenced and includes one-on-one work with requesting economies to develop appropriate cyber crime laws and cyber crime investigation units to work cooperatively with units in other economies. The Philippines, Indonesia, Thailand, Viet Nam, Chinese Taipei and Peru requested training. Training has been delivered to the Philippines and Indonesia and all training is expected to be completed by the end of 2004.



APEC members have been working toward establishing and raising awareness of the need for Computer Emergency Response Teams (CERTs), as well as developing guidelines for their establishment and operation. This project is designed to help economies establish the comprehensive legal frameworks and specialist institutions necessary to enhance e-security and combat cyber crime. APEC-funded training has been provided to Chile, Peru, and Mexico. Russia and Australia have funded training in Papua New Guinea, Vietnam, the Philippines, Indonesia and Thailand. APEC members are also developing a communications framework to facilitate a global CERT network. It is expected that all APEC members will have established or been trained to develop CERTs by July 2005.

### Counter Terrorism Task Force (CTTF)

The CTTF, established in February 2003, is APEC's primary oversight body for secure trade and counter terrorism activities, including implementation of the STAR agenda. The CTTF:

- assists economies to identify and assess counter terrorism needs;
- oversees the implementation of an APEC Counter Terrorism Action Plan;
- coordinates regional and bilateral capacity building and technical assistance programs;
- cooperates with international and regional organisations such as the International Maritime Organization (IMO), the World Customs Organization (WCO) and the International Commercial Airline Organization (ICAO); and
- facilitates cooperation between APEC working groups and committees on counter terrorism issues (APEC Secretariat, 2003).<sup>11</sup>

The CTTF was formed following the 2002 *Leaders' Statement on Fighting Terrorism and Promoting Growth*, and as such, is focused on implementing Leaders' priorities outlined in this document, including the STAR initiative. In the 2003 Leaders' Statement, APEC Leaders noted that there can be no prosperity without security and expanded APEC's security agenda to include commitments to: dismantle transnational terrorist groups that threaten APEC economies, eliminate the threat posed by weapons of mass destruction, strengthen domestic controls on Man Portable Air Defence Systems (MANPADS) and confront other direct threats to the security of the region (APEC, 2004). The CTTF has consequently evolved and is now considering strategies to not only consolidate existing efforts – focusing on the secure trade (STAR) agenda – but also to incorporate new and emerging priorities into its work program.

### Conclusion

As APEC economies represent around half of world trade (APEC, 2004), their security impacts directly on regional and global economic outcomes. Regional prosperity and growth is therefore inextricably linked to successful cooperative efforts to deal with terrorist threats, as open markets cannot thrive in an environment of insecurity.

---

<sup>11</sup> Other APEC working groups and committees working on counter terrorism issues include the Finance Ministers' Process, the Transportation Working Group, the Informal Experts Group on Business Mobility, the Sub-Committee on Customs Procedures, ECOTECH for capacity building, e-APEC and the Energy Working Group.

Through the STAR initiative and the work of the CTTF, APEC members have achieved a great deal to protect trade and persons in transit along with related financial flows. Despite this, much work is ongoing and more remains to be done. Continued assistance with capacity building should be encouraged for some time to come. This will assist the refinement of processes to maximise the benefits of shared ideas and experiences, and will ensure minimum disruption to trade.



## Chapter 3

### Experiences and Lessons Learned – Best Practices

This report looks in detail at five case studies of secure trade activities and projects undertaken in the APEC region, covering most aspects of the STAR agenda (see Appendix A for full case studies) in order to identify best practices so that the design and development of future projects might be improved. The first criterion for the selection of case studies was, of course, their contribution to APEC's secure trade objectives. A brief outline of this contribution is as follows:

#### APEC Secure Trade Objectives

##### *Maritime Security*

- STAR-Bangkok/Laem Chabang Efficient and Secure Trade (BEST) Project for container cargo security

The main benefit of BEST is its capacity to lower the probability of a terrorist attack utilising shipping containers, by improving monitoring and tracking processes. Other trade facilitation benefits include: greater overall efficiency, reduced stock requirements, improved in-stock rates, lower bill of lading surcharges, fewer theft incidents, reduced insurance and problem resolution costs, improved container tracking, and improved customer service.

- Chile's Graficación Marítima (GRAFIMAR) geographical information system for maritime security

The GRAFIMAR system works to protect maritime trade, especially through reducing terrorist risks to people and assets by improving the Chilean navy's capability to project its presence in the maritime and port fields. It also allows the Chilean navy to carry out port and shipping control and monitoring more effectively and to better coordinate responses to emergencies.

##### *Aviation Security*

- Karsof™ Total Airport Security System at Kuala Lumpur International Airport (KLIA) using biometrics for airport security

The Karsof™ Total Airport Security System enhances airport security by establishing a secure environment through the use of a specialised biometrics technology using fingerprints that identifies authorised visitors for entry to restricted areas. It also standardises security enforcement across the airport facility.

##### *Human Security & Business Mobility*

- Australia's Advance Passenger Processing (APP) system for business mobility and human security

The APP system ensures that persons who are not authorised to enter Australia are prevented from boarding flights and vessels bound for Australia. Advance Passenger Processing (APP) is Australia's version of an Advance Passenger Information (API) system. API systems provide border agencies with advance notice of a passenger's arrival on a particular flight or vessel.

### *Anti-Terrorist Financing*

- Indonesia's anti-money laundering (AML) and anti-terrorist financing (ATF) regime, particularly its financial intelligence unit (FIU) for halting terrorist financing

Indonesia's AML/ATF regime assists in preventing terrorist financing by criminalising it. It stipulates that the proceeds of terrorism and assets used for terrorist activities can be frozen, seized and confiscated. The AML/ATF regime also assists in preventing terrorist financing by providing for sanctions against money-laundering and by increasing the integrity and credibility of the financial system.

### **Emerging Themes**

Security is important to encourage and to protect gains in trade and investment liberalisation and facilitation. One way for economies to improve security is to learn from the experiences of those counter terrorism projects that have been undertaken. These case studies were provided by a cross-section of APEC economies and each covers a different aspect of the STAR agenda. Nevertheless, they exhibit similarities in terms of how they managed often significant changes to systems and processes, to enhance security and achieve greater trade and investment facilitation. There is therefore merit in exploring these studies for lessons learnt and to see how comparable issues were addressed.

While economies at different stages of development and varied levels of resources will approach projects in different ways, the general themes, as well as 'best practices', that emerge from the case studies should be considered by economies looking to introduce their own secure trade measures.

### *Trade Facilitation and Efficiency*

In addition to enhancing security, all activities analysed in the case studies result in other flow-on benefits through the efficiencies they create. The BEST project, for example, adopts an approach that improves security for goods all the way through transit. This is achieved by improving customs and supply chain operations, while also facilitating trade through: greater supply chain visibility; transparency and process improvements (e.g. increased transparency through container tracking); reduced customs inspection and minimisation of other delays; lower insurance charges; and reduced rates of theft.

Chile's GRAFIMAR system's major aim is to protect maritime trade and reduce risks to people and assets. However, it also allows the Chilean Navy (that has responsibility for port control) to carry out port and shipping control in a more effective and coordinated way by allowing reliable and timely information that facilitates operational duties on board vessels and at port, thus facilitating trade. It is also effective in coordinating responses to emergencies and other contingencies.

The main aim of Malaysia's Karsof™ biometric airport security system is to provide security and safety to airport users by allowing only identified and authorised users and visitors to enter restricted areas. At the same time, it also supports KLIA's stature as Malaysia's premier gateway, supports its aim to achieve a regional hub status by increasing security, and has created domestic expertise in the new technology.



The main aim of Australia's APP, as with all advance passenger information systems, is to improve security by only allowing people to travel to and enter Australia where they have a legal entitlement and where it is in the public interest. It also contributes to APEC's trade and investment facilitation agenda by enhancing the mobility of genuine business people by facilitating people movement in a more efficient way. It follows that this benefits passengers by reducing processing times and provides convenience at check-in for airlines.

Indonesia's AML/ATF regime has the objective of meeting international commitments on halting terrorist financing, which turn increases credibility of its financial system and confidence in the economy. It could also assist in having Indonesia considered for removal from the list of Non-Cooperative Countries and Territories and thus reduce the risk premium for Indonesians undertaking international transactions, lower overall costs to the economy.

#### *Demonstrating Benefit*

The flow-on benefits from implementing secure trade measures, such as the ones highlighted above, can play an important role in convincing stakeholders to introduce them. Stakeholders can be reluctant to implement secure trade measures where implementing them means that they face the imposition of different or extra burdens and tasks or a change to systems. If it can be demonstrated that there are additional efficiency benefits to the security benefits of introducing such measures, then stakeholders are more likely to implement them.

The BEST project, for example, involves effort by and extra costs to exporters from the introduction of new and specialised equipment to track containers, such as the RFID tags and readers. The company supplying the equipment found that where exporters received information on how the technology would facilitate trade, e.g. by allowing a container's progress to be measured via the Internet, they saw its value and were more likely to support it.

For the introduction of the Karsof™ Total Airport Security System, some staff were reluctant to adopt a biometric identification system because of the newness of the system and the sense that it imposed a rigid structure on staff that was unfamiliar. Airport management handled this by instilling confidence in users through tools such as a post implementation review, training sessions, education forums, a staff survey and making it clear that policies would be enforced by management.

#### *Strong Planning*

All projects, particularly those involving the introduction of new technology, require strong planning to ensure success. This planning should cover both the development and implementation stages.

The BEST project required a high level of planning involving a number of stakeholders on two continents, to decide the structure of the project and then follow-up to ensure the tight timetable was met.

The Chilean Directorate General of Marine Territory and Merchant Marine (DIRECTEMAR) applied strong planning processes to develop the GRAFIMAR system, based on standard procedures. These were to ensure that an application was developed in compliance with a set of regulations that reflected the objectives of the project. The development process was flexible in that it could occur through centralised or decentralised means. DIRECTEMAR had specialised personnel to control the modification process and used working groups of relevant personnel which coordinated with the user-administrator to make changes to the platform. The need to incorporate greater feedback from internal users into the development process became more apparent as the GRAFIMAR system added more complex data to its design, and its client base expanded. This need will be factored into future planning.

The Karsof™ airport visitor identification and authorisation system, based on fingerprint biometrics, was a major change to KLIA's security system. Using biometrics is a relatively new field, thus the system required development and testing. The private company contracted by the government to provide the system found that its successful implementation required a strong plan covering all aspects of the functional and operational system. The system development plan, which also helped to manage obstacles, involved user requirement analysis, strategies for customer acceptance, system development, adequate (internal and external) training, enforcement strategies, a post-implementation review and an inbuilt capacity for fine tuning. The post-implementation review was an important planning tool to ensure that the security objective was met, identify users' difficulties and to incorporate solutions in developing newer versions.

Australia's APP system case study demonstrates that planning is key to the successful introduction of new border security approaches. In particular, it highlights that key stakeholders and partners need to be involved in all planning activities from an early stage, including in developing systems specifications and implementation programs. For example, the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) worked closely with airlines to ensure that their systems interface with the APP system. The system provider in particular worked extremely closely with DIMIA staff to manage system change processes, from the earliest stages of system implementation through to undertaking user acceptance testing with airlines.

Indonesia's AML/ATF regime demonstrates that planning is not only necessary for new technology systems, but also for laying down appropriate legal and administrative frameworks – in this case to halt terrorist financing. The Indonesian Financial and Transaction Reports and Analysis Centre (PPATK) has worked to ensure that the right procedures are established to receive, process, evaluate and disseminate suspicious transaction reports in an effective and timely manner. Timeliness was found to be crucial in preventing financial flows to terrorist organisations and individuals, and was a key consideration in PPATK's planning.

#### *Flexibility and Capacity for Change*

The capacity to amend, change and further develop systems to account for experience and new information on evolving needs should be built into any secure trade project.



The ability to incrementally improve a system to provide a securer environment was an effective tool, particularly for those case study projects that built on previous work. Also, for the case study projects that implemented new security systems, the ability to include the means to adapt the systems to unforeseen circumstances was important in ensuring ongoing security and achieving flow-on benefits.

### **Project Development and Enhancement**

The STAR projects in the case studies have been enhanced and developed over time to take account of changed circumstances, to refine processes and to utilise new technology. This has resulted in improved security and increased flow-on benefits.

GRAFIMAR was developed to cope with different situations affecting its performance. When implementing GRAFIMAR, the major difficulty was users' lack of computer science education. This was overcome with methods such as using open standards and a single window concept to ensure information gathering and the collection of consistent and accurate data. Also, as the cost of software licences to fulfil expected demand for the system was likely to be high, DIRECTEMAR decided to focus future development of the system on the web platform. Another difficulty was that, although the shipping industry had been increasingly adopting information technology in its business processes, these were not fully compatible with the computing processes of the Maritime Administration. This demanded a standardisation in the electronic exchange of information, requiring that resources be directed to the development of computer tools to allow data exchange, regardless of the software being used.

A key part of the planning and implementation of the Karsof™ biometric security system was testing the system and the post-implementation review. As a result of these processes, user difficulties, network control and maintenance issues were identified and solutions found within a short timeframe. These included solutions to avoid physically monitoring every location throughout a vast airport; enable network monitoring staff to act pre-emptively against possible outages; improve response times for user problems; enable backup to be used for business continuity; and strengthen equipment to deal with vandalism.

Australia's APP system has been developed and extended over 15 years so that in June 2003 it covered 97 per cent of air arrivals, up from 65 per cent in the previous year, significantly improving security. A significant enhancement occurred from the beginning of 2004 when information on passengers on international cruise ships, along with ship and aviation crews, was included in the APP system.

### **Future Enhancements**

The case studies show that it is particularly important to be forward-looking when planning such projects, so that enhancements can be made at a later date to make the system better and more effective.

For example, DIRECTEMAR plans to further develop the GRAFIMAR system so that data from private and public entities is continuously integrated and so that sensors can be incorporated to improve control, surveillance and reconnaissance capabilities.

KLIA plans to enhance its biometric security system to collaborate with immigration, other government agencies and law enforcement databases to vet personal backgrounds. The system will also be extended to cover all security check points at the airport. A key future task awaiting approval is to make the system applicable to passengers.

In the case of Australia's APP system, efficient passenger mobility will be maintained, despite expected increases in passenger growth. Border agencies, airlines and airport owners will work together to ensure the APP system continues to deliver tangible and measurable benefits. Australia's border agencies will also work closely with international airlines to enhance the functionality and capacity of the APP system to ensure that it meets both the needs of airlines and government. In addition, the Australian Customs Service is working on a program to access and evaluate information held in airline reservation systems to enable it to identify in advance passengers who are linked in some way to certain risk criteria (terrorism, drugs etc.) and those passengers would be referred for further assessment on arrival at the border. Customs is working on achieving 100 per cent coverage of airlines flying into Australia. Another benefit of this system would be that enforcement operations at airports would become more streamlined, allowing resources to be deployed more effectively.

Indonesia's Financial Intelligence Unit (FIU), established by its AML/ATF legislation, plans to take advantage of information and communications technology by switching to an almost entirely electronic submission system when the relevant computer infrastructure is in place. This should raise efficiency and reduce costs for financial sector provision of reports. In addition, to make the analysis more effective, the FIU expects to move from manual analysis to using computerised analytical programs and to obtain specialised training in forensic accounting.

#### *Stakeholder Interaction*

The case studies demonstrate that introducing and implementing secure trade measures can involve a large number of players horizontally and vertically through the supply chain. This requires a high level of coordination and cooperation to ensure that new systems and processes are applied effectively. Generally, for project development of secure trade measures of the type covered in the case studies, it is important to create a strong public/private partnership. In particular, as pointed out in the BEST case study, the 'public and private sectors need to work together to avoid the public sector instituting a bureaucratic process such that companies are discouraged from putting forward ideas that would assist with achieving APEC's goals'.

#### **Coordination and Cooperation in Project Development**

Most of the secure trade projects examined in the case studies involved intra and inter governmental coordination across a range of areas. For some projects that used information technology intensively, private sector operators provided the technology or maintained the systems. These case studies showed that it was necessary to maintain close cooperation with key stakeholders and for the private and public sectors to work together seamlessly.



For Australia's APP system, the government agency, a private provider and an international association cooperated to achieve the desired outcome. These stakeholders worked together so that they had input to the system which, in turn, minimised disruption to their processes and ensured an efficient and effective outcome. The APP system has been developed incrementally as DIMIA's business requirements have changed and Australia has worked closely with airlines to address these changes. The cooperative relationship with airlines and other stakeholders has been a fundamental feature of the development and implementation of each phase of APP.

The BEST project involved three private sector exporters and some other 'private' entities, as well as a wide range of public agencies. These stakeholders worked together closely to ensure outcomes were achieved in a very short time.

Cooperation in project development also assists with effective uses of new systems. For example, with the Karsof™ system, the collaboration between (aviation security) AVSEC, human resources and technical personnel in supporting the post-implementation of the biometric airport security system provided a guideline for enhancements in the system that was able to take into account user needs and those of all stakeholders.

In the case of Indonesia's establishment of an AML regime, the Indonesian Government's cooperation and consultation with the financial service providers helped overcome their resistance to supplying additional information, which ultimately related to the government's ability to impede terrorist financing.

### **Coordination and Cooperation in Operation**

The case studies also demonstrated that the public-private and other stakeholder interaction can be important in the application of the new systems. Chile's Maritime Authority found that GRAFIMAR's successful operation relied on good cooperation between stakeholders. The interaction between the public and private actors in the system's processes was based on reliable partnerships, requiring all actors to work towards one common goal of promoting the nation's maritime interests. Chile's GRAFIMAR system relies on public-private interaction to input data in the system through the use of both automated and manual systems. DIRECTEMAR also has agreements with other public sector agencies to obtain data by electronic data exchange. To check accuracy of the data, it uses several validity methods.

Australia worked closely with airlines in implementing its APP system. The day-to-day operation of Australia's APP system relies on the support and input of international airlines. To ensure it operates effectively, Australia provides round-the-clock assistance to airlines in resolving difficult cases.

The cooperation on project operations can be formalised, particularly in an area requiring the exchange of confidential financial information. For example, for Indonesia's AML/ATF regime, ensuring that information could flow effectively between relevant bodies has been imperative to meet the goals of the regime. To achieve this, PPATK worked closely with other public agencies, on the basis of memoranda of understanding, and with the private sector through provision of detailed guidance on reporting.

### *Effective Use of Technology*

Advanced technology was shown to be an effective tool in improving security in most of the case studies. Four of the five case studies used information and communication technology to effect a tighter security regime, all finding significant net benefits from these systems.

- The BEST project used new, but increasingly widespread, radio frequency identification (RFID) technology for container security, allowing containers to be tracked through the supply chain.
- The GRAFIMAR system used electronic databases, the Internet and computer graphics to display in real time the location of ships in territorial waters.
- The Karsof™ airport security system used biometrics technology to restrict access to legitimate airport staff and visitors.
- The APP system used the global communications network to send advance information on international passengers.

The intensive use of information and communication technology in STAR projects means that accessing expertise in this sector is necessary to ensure that APEC's security and facilitation goals can be met. Chile's experience was that to achieve success in identifying and tracking shipping using a geographical information system, reliance on an information technology unit with a strong research and development ability was required in order to develop applications and to integrate various technologies. Other projects accessed information technology expertise from the private sector, maintaining close collaborative relationships with these organisations to ensure goals were met.

Utilising open systems also creates efficiencies for system developers and users. For instance, GRAFIMAR relies on open code software which is free, an important consideration given the large number of users of the system. The Karsof™ biometric airport security system also uses open source architecture to cater for technology growth, as it provides flexibility and removes constraints.

The use of existing technology and systems, where possible, can also be advantageous as it creates efficiency. Australia's APP system uses SITA's existing global communication network to link airlines' reservation systems with the government agency's immigration databases, ensuring the use of already proven technology, while avoiding expenditure on new infrastructure.<sup>12</sup> Using the SITA network also benefits airlines, as they are able to develop their own interface to be compatible with the SITA network, giving their staff the best possible interface.

For best results, information technology systems should interface with external systems. GRAFIMAR's open code system has made it possible to 'establish relations with public and private organisations using the single window concept, tightening the processes and increasing control'. The Karsof™ system's open architecture also allows it to interface with external systems, such as enforcement agencies, for online verification.

---

<sup>12</sup> SITA, originally called the Société Internationale de Télécommunications Aéronautiques, is an international association providing data and telecommunications services to the international airline industry ([www.sita.aero](http://www.sita.aero), accessed 29 July 2004).



A user interface should be as simple and as clear as possible. Australia's APP system, in allowing airlines to develop their own interface to the SITA network, enables them to develop the interface such that it is suitable for their business and staff to use. The Karsof™ security system also has the major benefit of being easy to use, 'taking little time and effort' to provide fast and reliable identification. The system underpinning the BEST project allows containers to be tracked without further human intervention after they have been filled and sealed. Relevant parties can then easily access the database to determine the status and location of the container.

### *Education and Capacity Building*

Education and training are vital components of all the projects studied, allowing new systems to be introduced with a minimum of changeover cost. This component is particularly important with the use of high technology tools.

Education and training should be included as part of the strategic planning for the development and implementation of the project. It was a major component of the Karsof™ project; the service provider provided specific training for KLIA personnel to operate and maintain the system.

For GRAFIMAR, education and training was provided every time that a new application was released, with the Information Technologies Department and the user-administrator jointly planning the way in which the instruction will be carried out to ensure its efficacy, and personal records were kept to ensure all users had the relevant training.

Education and training should be aimed at both internal and external users, as appropriate. For example, education and training was also provided to the external users of the GRAFIMAR system.

System documentation, including users' guides, are useful tools to enable users to find information on straightforward issues quickly and easily. This was an important tool for the GRAFIMAR system and the Karsof™ biometric airport security system.

The case studies demonstrate the benefits of using new technologies to provide training and system information, as well as user feedback mechanisms. For the BEST project, project training courses were delivered successfully over the Internet. The GRAFIMAR system also employed an on-line manual and the user-administration used an e-mail address for suggestions for amendments or modifications.

Particular emphasis should be put on education and training where staff need to undertake new specialised tasks. For example, Indonesia's FIU ensured that, in introducing the new AML/ATF regime, it provided training to build, develop and increase the capacity and effectiveness of its personnel.

### *International Cooperation*

International cooperation is a fundamental requirement to fight terrorism effectively due to the high cost flows between economies from a terrorist event and the large public benefits that can be gained from working together. The cooperation can take several forms: specific cooperation between economies to implement a defined project;

multilateral cooperation to develop standards or general principles in a particular counter terrorism area; an economy seeking international assistance (for example in capacity building); or economies cooperating to exchange relevant information to improve security.

The BEST project provides a good example of two economies working together to achieve end-to-end supply chain security for container trade. This involved the private service provider and the project managers working with Thai authorities to set up and use equipment, and with Thai exporters to take part in the demonstration.

It was also found in the case of the APP case study that cooperation with relevant international fora can be a key element in a successful project, particularly in developing and promulgating standards and building of existing international efforts. For instance, Australia's APP has been developed in line with global Advanced Passenger Information (API) systems and related standards, to ensure interoperability and compatibility of the system with other API systems. In developing its system, Australia has worked closely within the International Air Transport Association (IATA) and with other APEC members on technical issues to allow electronic exchange and confirmation of passenger data between economies' systems, as well as interactive document and alert checks. Australia noted that 'by cooperating on technical issues, the use of API systems will increase and the savings will be magnified'.

International cooperation to build capacity can be especially useful where new staff skills in specialised areas are necessary. Indonesia's FIU found that, to improve capacity, its personnel benefited greatly from international expertise provided by a range of agencies. Benefiting from other economies' experience and expertise meant that multilateral rules and guidelines could be applied with a minimum of difficulties.

#### *General Application to Other Economies*

Due to the highly technological nature of most of the secure trade solutions analysed, many developing economies with shortages in resources and skills are likely to face some level of difficulty in implementing them. (Capacity building measures can go some way in addressing these gaps.) Ultimately, however, similar lessons should apply.

The systems/measures discussed in the case studies have already been tested. As such, problems or difficulties have already been identified and solutions offered to improve them. Significant time and funds are spent on the testing phases of such systems/measures. Developing economies that choose to adopt similar systems/measures to those described in the case studies should, therefore, be able to adopt them at a lower cost than the original economies did. For example, the features of the Karsof™ system, some of which were developed as a result of a post-implementation review, such as increased user friendliness and relatively low implementation and infrastructure costs (compared to other technologies), should enable easier implementation in other airports.

The application of GRAFIMAR to other economies is specific, as DIRECTEMAR aims to make the system available to other economies so as to improve their maritime security activities and permit joint operations, which contributes to the STAR APEC objectives.



## Summary

In conclusion, the case studies show that the same lessons apply in enhancing the effectiveness of a secure trade measure and maximising the efficient use of available resources, regardless of the measure or the economy implementing it. Features of successful projects that aim to secure trade are:

- demonstrable benefits, both in terms of improved security and efficiency, to stakeholders and users;
- strong planning evident in each stage of project cycle;
- flexibility and built-in capacity for change at a minimal resource cost;
- strong stakeholder interaction, including between the public and private sectors;
- where relevant, the effective use of available and new technology;
- strong education and capacity building components;
- capacity to expand to other economies/interoperability; and
- international cooperation.



# Chapter 4

## Conclusions

Implementation of secure trade measures, particularly through effective cooperation, can lead to long-term economic efficiencies. The Secure Trade in the APEC Region (STAR) initiative demonstrates this and underscores the importance of facilitating travel and trade, while enhancing our security.

The STAR initiative has achieved much in a short time, covering its main areas of focus: aviation security; maritime security; business mobility and human security; combating terrorist financing; and promoting cyber security. It has also made progress in monitoring implementation and has provided broad and varied capacity building to APEC economies that require it. As a result, the STAR initiative has encouraged greater cooperation among economies, provided for development of regional responses and has shared the costs of secure trade measures across the region.

This report analyses five case studies of projects undertaken under the STAR initiative, involving both developed and developing or middle income APEC economies. It distils ‘best practices’ and general principles that APEC economies should take into consideration when developing and undertaking similar counter terrorism activities.

## General Principles and Best Practices from the STAR Initiative

Most of the best practices derived from the analysis of the case studies of STAR activities are common to all projects analysed. Therefore, they have general application to the development and implementation of most secure trade measures, particularly those involving the use of advanced technology.

The best practices or general guidelines for economies introducing and implementing new secure trade measures are listed below.

- Governments need to be committed to introducing and applying the measures and focus on outcomes.
- Trade facilitation and other efficiencies are concomitant parts of an increased security regime; this helps to ensure that all stakeholders have an incentive to follow the regime.
- The demonstration effect of the individual benefits to stakeholders can be a powerful tool to gain commitment to secure trade activities.
- Strong planning, especially when the introduction of new technology is involved, is required at both the development and implementation stages, to ensure success and to overcome obstacles.
- The capacity to amend, change and further develop the systems to account for experience should be built into projects.
- Projects should be able to be enhanced and developed over time to make allowances for changed circumstances, to refine processes and to take account of new technology.
- Projects should be forward looking so that enhancements can be easily made to make the system better and more effective.

- A high level of coordination and cooperation between and with stakeholders should be built in to ensure that new systems and processes can be applied effectively; this also creates ownership in the process.
- It is necessary to maintain close cooperation with key stakeholders and for the private and public sectors to work together seamlessly.
- Information and communication technology is an effective tool in achieving stronger security, resulting in significant net benefits, even when the economy concerned has limited capacity in terms of equipment and expertise.
- If projects rely on technology, the necessary expertise should be accessible and/or the required skills should be developed to maintain it.
- The use of open information technology systems creates efficiencies for system developers and users.
- The use of existing technology and systems, where possible, creates efficiencies by avoiding the need to invest in new infrastructure.
- Where information technology systems rely on external information, they should be able to interface with external systems.
- Where possible, the user interface of a information technology system should be simple and clear.
- Education and training:
  - are vital to establishing new systems with a minimum of changeover cost; this is particularly important with the use of high technology tools;
  - should be included as part of the strategic planning for the development and implementation of the project;
  - should be aimed at both internal and external users; and
  - should be particularly targeted where staff need to undertake specialised tasks.
- System documentation, including users' guides, are useful tools to enable users to find information on straightforward issues quickly and easily.
- Good management is key to ensuring that users' acceptance and education is effective; management plays a major role in identifying users' requirements, evaluating the system's appropriateness and enforcing the system.
- In order to fight terrorism effectively, it is necessary for the international community to cooperate on the development of common systems/arrangements and standards so that:
  - costs can be contained;
  - duplication of systems and/or training can be avoided;
  - spill over benefits are demonstrated and communicated;
  - interoperability is ensured; and
  - capacity building assistance can be provided where training in new skills or specialised area is necessary.



- While developing economies are likely to face some level of difficulty in implementing security measures due to cost and skill issues, as the systems have already been tested and improved upon by other economies, developing economies should be able to apply the measures at a lower cost.



## APPENDIX – CASE STUDIES

### PORT SECURITY

#### A1 – Container Cargo Security – STAR–Bangkok/Laem Chabang Efficient and Secure Trade Project (US/Thailand)

##### Background

In February 2003, the National Center for APEC began developing a pilot project to test concepts and technologies for implementing an end-to-end supply chain security system, known as the STAR Bangkok/Laem Chabang Efficient and Secure Trade (BEST) project.<sup>13</sup> In August 2003, the US Trade and Development Agency awarded a US\$500 000 grant to the Ministry of Foreign Affairs of the Government of the Kingdom of Thailand to support the project. The private sector, working through the National Center for APEC, played a key role in this project, working to improve supply chain security through enhanced transparency and information processes. These processes also facilitated trade and achieved cost efficiencies.

The BEST project promotes both security and trade efficiency through its central component of the use of electronic seals and other technologies. It uses radio frequency identification (RFID) and electronic seal (e-seal) technology to transmit information via satellite (in real time) about goods in transit between ports in secured containers. This has required the installation of transmission and reception equipment at the transshipment points and the port, providing handheld readers to exporters and importers and provision of e-seals to be placed on the containers.

The project was implemented over August and September 2003 in a trial involving a total of 30 containers sent from Laem Chabang, Thailand's primary international port located south-east of Bangkok, to the Port of Seattle in Washington State on the north-west coast of the United States, through ports in Taiwan and Korea. Laem Chabang handles more than 3 million outgoing containers per year; of these, 20 000 containers are shipped from Laem Chabang to Seattle.<sup>14</sup> Goods transported to Seattle are mainly products such as electronics, toys, canned tuna, clothing and auto parts (BearingPoint, Inc., 2003).

##### Objectives

The BEST project's goals were to strengthen US-Thai economic relations, facilitate international trade, enhance Thai trade competitiveness, increase business confidence in trans-Pacific trade lanes and deter terrorist attacks. A key objective was to improve customs and supply chain operations, building on previous security initiatives with related objectives such as Smart and Secure Tradelanes (SST), Operation Safe Commerce (OSC), the US Customs Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT). In particular, the BEST Project aimed

13 The National Center for APEC aims to generate and stimulate US support for and participation in APEC. It works closely with the US Coordinator for APEC and other US Government agencies to encourage and facilitate broadly based US private sector involvement APEC's activities, its Working Groups and other APEC-related bodies, and serves as the secretariat for the three US members of the APEC Business Advisory Council (ABAC) ([www.ncapec.org](http://www.ncapec.org), accessed 13 August 2004).

14 Thailand's total container cargo trade to Seattle each year is around 600 000 containers (BearingPoint, Inc., 2003).

to test the technical feasibility and to evaluate the financial feasibility of establishing a secure supply chain.

### Box A1 BEST Project's Costs and Benefits

Shippers will face costs and benefits from the introduction of a secure end-to-end supply chain as trialled under BEST.

- Costs include the cost charged per container by the service provider to earn income to cover the initial investment in the new technology (planning, designing, configuring and installing hardware along with the cost of the hardware (RFID tags, handheld readers and signposts)) and the ongoing network operating and maintenance costs. The estimated costs are a one-time cost for infrastructure of US\$0.44m, a one time implementation cost of US\$3.43m and operating costs which include an annual cost of US\$0.1m plus a cost per container of US\$86.
- Benefits result mainly from greater supply chain visibility, transparency and process improvements. They include greater efficiency through lower customs service inspection rates and fewer related delays, reduced stock requirements and hence inventory carrying costs, improved in-stock rates, lower bill of lading surcharges, fewer theft and pilferage incidents, reduced insurance costs, improved container tracking, lower problem resolution costs and improved customer services.

Further, a wider public benefit arises from increased security and the lower probability of a terrorist attack utilising shipping containers.

Cost benefit analysis of the project found that the security solution is financially feasible.<sup>15</sup> In fact, companies importing goods into the United States should realise impressive financial benefits:

- aggregate benefits range from US\$150 to US\$2 000 per container
- adjusted conservatively for uncertainty and risk, the benefits will exceed US\$220 per container with an 80 per cent probability
- the break even solution for this trade lane is 8 000 containers based on the US\$220 cost per container.

Thai exporters face an estimated cost of US\$50 per container, however this may be less as e-seals can be re-used. The benefits for Thai shippers or manufacturers are more difficult to estimate, but would include a higher level of competitiveness through higher security, supply certainty and trade efficiencies.

Source: BearingPoint, Inc., 2003 and Pacific Economic Cooperation Council Network, 2004.

## Implementation of the BEST Project

The project's secure end-to-end supply chain between the two ports involved establishing security protocols, business procedures and the installation of a supply chain security and tracking solution, as well as capacity building efforts to train shippers, port operators and public officials in the new systems and procedures (BearingPoint, Inc., 2003).

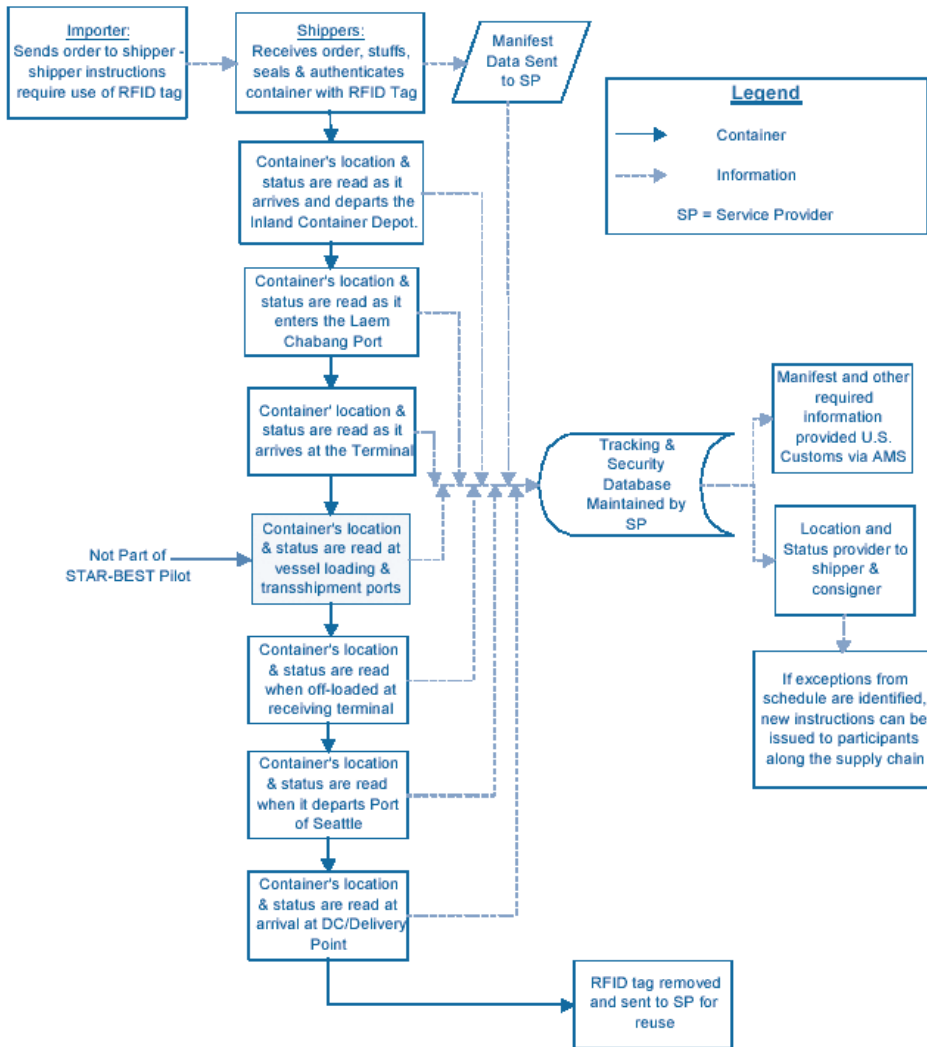
The basis of the technical solution to achieve end-to-end supply chain security is an active RFID tag which is designed to fit on an ISO standard bolt.<sup>16</sup> It is activated when a container is stuffed and sealed at an exporter's facility. As the container moves through the supply chain, the tag broadcasts the container's status and location to

<sup>15</sup> This cost benefit analysis did not take account of public benefits and assumed a single entity designs, deploys and operates the required infrastructure and networked information systems and charges shippers a per container fee to utilise the network.

<sup>16</sup> The chip is now estimated to cost 15-20 US cents a piece, but some indicate the price could fall to 5 cents each by 2005. RFID tags can hold 128 bytes of information, compared to 1.1 bytes in a bar code and unlike bar codes RFID tags can be read without a line of sight.

a series of readers and signposts positioned at key checkpoints. The tag notifies the system immediately if the electronic seal is broken or removed. The container's status is updated in real time onto a secure database which gives confidence in the reliability of a container's manifest and allows shippers to identify inefficiencies in the supply chain and pass the order status to customers (Figure A1).

Figure A1 BEST Project Process Map



Source: BearingPoint, Inc., 2003.

The project involved containers from three separate exporters (a tuna processor, a large consumer electronics company and a freight consolidator). Each container was stuffed, sealed and RFID-tagged after packing and each tag was programmed with shipment-specific information using a handheld reader after which the manifest was generated and sent. Containers were then moved by truck to a container depot, where they were loaded onto rail cars to go to the port. The depot had two signposts and one reader to track each container's arrival, handling and departure. At the port, each container was reloaded on a truck, moved through a port gate and delivered to the appropriate terminal; readers were installed at a port gate and at a terminal. The containers were shipped to Seattle where the e-seals were checked and a reader at the receiving terminal recorded each container's arrival in Seattle and one at the port gate recorded its departure from the port. Then the containers were sent to their destination point where operators with handheld computers verified the containers' origin and contents and, once verified, receivers used the handheld readers to unlock the seals so the contents could be removed. Personnel using the system were authenticated using their individual log in ID.

## Key Lessons Learned

### *Strong Planning*

As with all project development, the BEST project required a high level of planning across two continents. United States and Thai officials met during the project consideration phase to discuss how to structure the project. The project also required follow-up on a myriad of issues to keep the project moving on a very tight timeline.

### *Stakeholder Cooperation and Public-Private Interaction*

Cooperation between all stakeholders in the project was a key to its success. The project involved intra and inter governmental coordination across a range of areas. It covered many organisations from the private and public sectors, including the three exporters, road and rail transport and shipping companies, private companies which supplied and installed the equipment and provided training and other services, the National Center for APEC, agencies of the Royal Thai Government (the Office of the Prime Minister, Ministry of Foreign Affairs, Ministry of Transport and Communications, Thai Customs, the Port Authority and State Rail of Thailand), United States Government agencies (which supported the project, although not directly involved) (State Department, US Customs and the US Trade and Development Agency, the Port of Seattle) and private sector bodies (ABAC/CEO Roundtable, Airport Authority of Thailand and the Thai International Freight Forwarders Association).

For project development of this sort, it is important to create strong public/private partnerships to achieve goals. The public and private sectors need to work together to avoid the public sector instituting a bureaucratic process in such a way that companies are discouraged from putting forward ideas for projects that would assist with achieving APEC's goals.

The company supplying and installing the equipment found some bottlenecks in the process. It consulted Thai Customs for importing the required equipment, the Thai



Department of Post and Telegraph for approval to operate radio frequency equipment and the Port Authority of Thailand for approval to install equipment on port land. The company found that, to facilitate future such projects, streamlining the import procedures for equipment needed to secure trade would be helpful. Also, as RFID requires the use of radio frequencies, it would be useful if the APEC economies would assign and license frequencies for these uses.

Good relationships and strong communications within the private sector were also imperative. The RFID solution required effort on the part of exporting firms, explaining the difficulties that were experienced in finding shippers to participate in the demonstration; these firms may not immediately see the benefits whereas the costs will be obvious. Exporters may be concerned that the technology will be required for all goods exported to the United States and that they will be forced to pay for this. However, the technology provider found that where exporters received information on how the technology will facilitate trade, for example by allowing a container's progress to be measured via the Internet, they saw its value.

#### *Education and Capacity Building*

The STAR/BEST project's educational component, which aimed to help cargo carriers and logistics service providers comply with US Customs requirements, specifically the 24 hour manifest rule of the Container Security Initiative, differentiates it from other security tracking initiatives. To deliver the project training courses, a US-based technology firm adapted its Internet educational platform with existing and new materials.

The system supplier did not face much difficulty in installing and teaching operators to use the system, however language was an initial barrier. The supplier overcame this by using a local partner. When training operators, the company was able to find in reports the various functions and roles that the different operators perform as part of SST (an industry-driven supply chain security initiative), enabling them determine the appropriate scope of training. Generally, with fixed instrumentation, the terminal operator and transport operator require the least training as compared to the party that fills and seals the container.

#### *Effective Use of Technology*

By employing new, but increasingly adopted, technology, the BEST project was able to demonstrate cost efficiencies, whilst also facilitating trade. The technology creates efficiency by achieving outcomes required by US agencies. BEST's sophisticated tracking methods can meet the US '24 hour rule', that requires carriers to report the contents of containers and other data 24 hours prior to loading in a foreign port. In addition, once the container is sealed there is a high probability it will not need to be checked by Customs after arrival in the United States.

#### *Promotion of Economic Efficiencies/Trade Facilitation*

The BEST project is an approach that improves security while also facilitating trade. It secures goods in transit rather than just securing the transport nodes and thus is a useful model for wider security measures.

## Conclusions

The success of this demonstration project should build confidence for exporters and consumers as it resulted in enhanced supply chain security in the region (APEC Counter Terrorism Task Force, 2004). The project demonstrated methods for supply chain security and efficient trade in the APEC region, which means it could serve as a model for broader application. It also demonstrated savings that could be made by utilising RFID technology to secure, track and manage supply chains more effectively as the assessed risk of a United States bound container being inspected is reduced as supply chain security levels were improved. Thus, successful implementation of such Electronic Data Interchange (EDI) schemes is an important way to facilitate trade and reducing the related costs.



# MARITIME SECURITY

## A2 – Chile’s GRAFIMAR System

### Background

The Directorate General of Marine Territory and Merchant Marine (DIRECTEMAR) of the Chilean Navy play a key role in the facilitation of maritime shipping and enhancement of maritime security through the Graficación Marítima system (GRAFIMAR) system – a geographical information system (GIS), which increases the capacity and efficiency with which Chile can monitor maritime traffic.

### Objectives

GRAFIMAR’s primary goal is to protect maritime trade, including through reducing terrorist risks to people and assets. The GRAFIMAR system has helped improve the role of the Chilean navy in port management and allows DIRECTEMAR to carry out port and shipping control more effectively and better coordinate responses to emergencies and other contingencies (DIRECTEMAR, 2004).

### The GRAFIMAR System

The GRAFIMAR system involves command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) (DIRECTEMAR, 2004). It allows the position of a ship at sea to be tracked on the basis of information provided by periodic ships’ reports and by satellite sensors. The source applications provide the data which is then integrated and changed into useful information for analysis and decision making to maintain maritime safety and security (Figure A2). The information is able to be displayed graphically in different real time dynamic global scenarios.

### *Applications*

DIRECTEMAR developed the GRAFIMAR system based on commercial software. The system has been established as a client-server architecture, i.e. it is installed in every workstation. Information requests (vessel, persons, cargo, position, location of the vessel, etc.) are sent from the central databases at Valparaíso to the relevant location.<sup>17</sup>

Through its graphical system, GRAFIMAR provides a real time picture of the exact position of all vessels in Chilean waters, allowing DIRECTEMAR to monitor shipping 24 hours a day. The graphical component of the GRAFIMAR system consists of graphics software and a cartographic database and uses open code.<sup>18</sup> The cartographic database is on a special server and uses a specific database management system with the operating system, so that the electronic maps are incorporated to the databases according to the details requested. To display data from external sources, GRAFIMAR uses web services technologies that facilitate the exchange of pre-defined and automated information, allowing for encryption if appropriate.

17 At present, the system has 1 700 personal computers and 84 servers distributed across Chile.

18 It uses a Java servlet and Java applet set up at the workstation allowing dynamic use of the system once the selected cartography has been loaded.

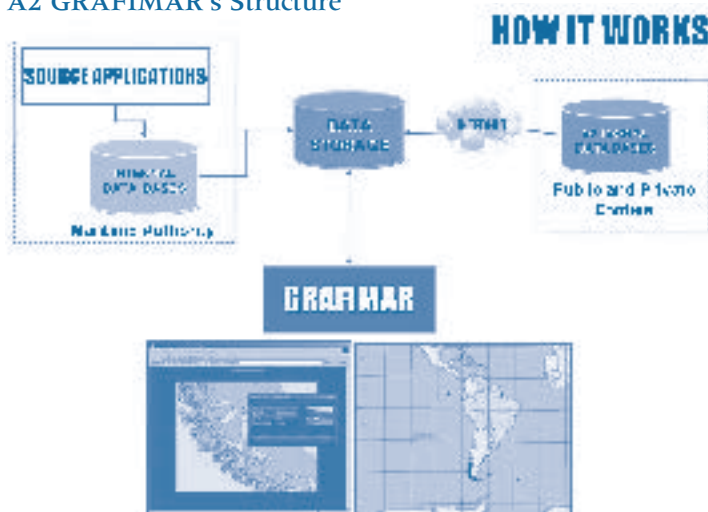
### Data

To activate the monitoring of a vessel through the GRAFIMAR system, data on vessels must be entered by the shipping agency, by the maritime authority, or by surveillance and reconnaissance identification. Once entered, the vessel is then monitored. To validate a vessel's position, the following data sources are used:

- the automated information system (AIS), by means of an automatic device of limited range;
- the vessel monitoring system (VMS) for Chilean industrial fishing vessels;
- a semi-automated system (LANTANO), that permits identification and tracking of a vessel while underway in certain areas using a specific software;
- a manual system (QTH) of voluntary position reporting of a vessel navigating within jurisdictional waters;
- aerial-maritime surveillance reports which permit identification and tracking of vessels as well as the manual adjustment of their estimated position; and
- maritime patrol reports which permit identification and tracking of vessels as well as the manual adjustment of their estimated position (DIRECTEMAR, 2004).

All data received is integrated, linked and updated in the databases. The databases have complete information on Chilean merchant and fishing vessels, while information on foreign vessels is constantly being stored as they call at Chilean ports.<sup>19</sup> The databases also include logistical information on port infrastructure and facilities for most ports. The information in the databases is complemented by using the Internet to access different databases worldwide, improving GRAFIMAR's dynamism and operability.

Figure A2 GRAFIMAR's Structure



Source: DIRECTEMAR, 2004.

<sup>19</sup> Data on the professional competency of Chilean people involved in maritime activities is also available in the databases using information obtained from DIRECTEMAR's authorisation role.

### *Communications Network*

Data is transported via an internal information network, called DATAMAR, a multiservice wide area network of national coverage based on internet protocol. DIRECTEMAR is therefore able to stay in contact with and circulate data centrally to its 16 local port authorities and 60 port captain offices. Maritime authorities can enter additional data. Currently, GRAFIMAR is only available on the DATAMAR network.

Since 1996, gathering information from maritime agencies and authorities has been carried out through the internet. The control of port facilities access is carried out via a web application which makes information available on people working at the ports. For port logistical information, the possibility exists to establish a internet connection between each port to allow access to additional information as well as access to their monitoring systems. Connection with the port of Valparaíso is presently under trial.

### **Future Developments**

Further development planned for GRAFIMAR is orientated towards continuous integration of data from private and public entities. DIRECTEMAR is developing systems to permit interaction with different sources at one time. Future efforts will also be focused on incorporating sensors to improve control, surveillance and reconnaissance capabilities. The capacity to include data on vessels equipped with AIS will soon be implemented so that their location and other details can be automatically displayed. Access to cargo manifests is now being considered by the Chilean Customs Service.

Another version of GRAFIMAR is being upgraded into a web version by December 2004. This will operate under internet protocols using open source tools. The difference between the current version (client-server) and the Web version, is that no additional software would be needed.

### **Benefits Achieved**

Since GRAFIMAR's implementation in 1995, it has been rated a reliable and useful tool by the national and international maritime community. The use of information technology to collect, analyse, interpret and integrate data and coordinate answers before emergencies and other contingencies arise makes it possible for DIRECTEMAR to better carry out the task of controlling marine and harbour traffic. The electronic exchange of information, its integration into databases and its interaction through the web creates further efficiencies in terms of operations on board vessels and at port. These system attributes have the effect of making trade more efficient, while the updated and graphical surface picture enables DIRECTEMAR to plan in advance the necessary action to meet security objectives.

### **Risks/Obstacles Encountered**

The major problem encountered in implementing GRAFIMAR was the lack of computer skills among its internal and external users. This compromised reliability and timeliness of information management and transmission. To remedy this quality assurance procedures were put in place in 1997 for the collation of information and to ensure its consistency.

Another major difficulty encountered was that the initial system had been created using commercial tools that did not easily allow for significant expansion of use. Specific limitations related to the client-server architecture and the related increase in cost of software licences as use of the system expanded. To solve this problem, it was necessary to improve the connection capacity of the internal DATAMAR network and, at the same time, to upgrade the architectural frame of GRAFIMAR to include the capacity for system upgrades as required and to meet future needs. This has been important as the shipping trade industry in Chile has increasingly relied on information technology to improve its business processes.

## **Lessons Learned – Best Practice Processes**

### *Stakeholder Cooperation and Public-Private Interaction*

The GRAFIMAR system's successful operation relies on good cooperation between stakeholders. In order to achieve effective interaction between public and private sector stakeholders, and their input into the processes managed by the Maritime Authority, all stakeholders had to adopt the common goal of promoting the nation's maritime interests.

Cooperation between the stakeholders is also essential for the GRAFIMAR project as the system is interactive and cannot operate without cooperation between authorities, ports and vessels. The accuracy and timeliness of the data input by each port office and by relevant external bodies needs to be ensured. This was achieved through several validity methods, and initially, by changing the structure of the databases to ensure that information was not duplicated. In most cases, this implied the use of IMO numbers and crew data. Information exchange was improved in 1996 when interaction between private and public organisations became possible via the internet. Maritime stakeholders could then enter information related to vessels and crew to achieve timely, reliable data. This technological integration made it possible to establish relations with public and private organisations under open standards using the single window concept. The system also has the added capacity to display vessels fitted with satellite positioning systems.

DIRECTEMAR also has agreements with other public bodies that allow it to obtain data by electronic exchange of information. The conceptual framework used is the single window that allows these entities to engage with the Maritime Administration, which then sends information on to other bodies exclusively as required, exclusively; a more streamlined process.<sup>20</sup>

When beginning the processing of relevant maritime data, some inconveniences affected the correct operation of GRAFIMAR. In 1996, the shipping industry's information technology systems were not fully compatible with the computing processes of the Maritime Administration. This required resources to be directed to the development of computer tools to allow data exchange regardless of the software being used.

---

20 The integration of public bodies began with the signing of conventions regarding the exchange of information among governmental entities, the first being the National Customs Service and the Registry Office, later including the Labour Inspection Office, the Civilian Police of Chile and other entities involved with the provisions established in the Convention on International Facilitation of Maritime Traffic (FAL 1965), such as the National Health Service and the Livestock and Agriculture Service.



### *Efficient Use of Technology*

The GRAFIMAR system extensively uses information and communications technology. DIRECTMAR's experience shows that the only way to successfully meet the challenges of identifying and tracking shipping is to rely on an information technology unit with a high research and development ability, capable of integrating various technologies to benefit the strategic goals of the administration. For example, DIRECTEMAR's Information Technologies Research and Development Unit were able to focus future development on the web platform, rather than a client-server architecture. Also, it decided that open code software would be used for its programming, meaning that it is free. This is important when considering the great amount of users that would access the GRAFIMAR system. At the same time, free development tools permit DIRECTEMAR to use and modify, when needed, the features of the incoming data and the display of information. This also allows, through the use of international information technology standards, the electronic exchange of information with any other economy requiring such information. A change to a website platform will further mean that, by using the DATAMAR network as the main mechanism to transfer information, any communication media that allows interaction with the internet will be able to access GRAFIMAR.

Efficiencies in data collection are also evident. The percentage of new data on ships required is declining because GRAFIMAR's database has information on all of the vessels that have called at Chile since 1995. If a vessel arrives to Chile for the first time, all the data must be registered. After that only entry updates regarding cargo, crew and certificates are needed. It follows that this process creates efficiencies in the management of maritime traffic. The development of relevant standards to ensure compatibility of information technology systems between industry and government was also integral to more efficiently facilitating maritime trade.

### *Education and Capacity Building*

GRAFIMAR is operated by nearly 2 000 people. Accordingly, education and training in the use of this high technology tool is key to its effective operation and use. Every time a new application needs to be released, the Information Technologies Department and the user-administrator jointly plan the way in which the corresponding instruction will be carried out, for both internal and external users. Training is undertaken at DIRECTEMAR's facilities in Valparaíso and/or at the users' place of employment. All the applications have an online manual, and the user-administrator has an email address for suggestions or amendments.

DIRECTEMAR's own personnel are trained in the use of the different applications at polytechnic schools or instructional centres, with skills being upgraded at least once every two years.

### *Strong Planning*

It was important for DIRECTEMAR to set clear objectives about what it was trying to achieve through GRAFIMAR from the outset. The development of every application needed to comply with the related regulations and guidelines for it to meet these objectives.

Application development is based on standard procedures that consider, among other things, its legality, determining exactly what is being sought, its required analysis from processes and other strategic requirements. The operational methods of the applications that are to be released are determined by the Maritime Administration and, depending on the case, are developed in a centralised or decentralised way.

DIRECTEMAR ensures that it has specialised personnel to control the modification process and uses working groups of relevant personnel which coordinate with the user-administrator in developing the required improvements and changes to the platform. As GRAFIMAR's use changed from that of a command and control tool for search and rescue centres to much broader use with a high level of detailed data, the need to incorporate greater feedback from internal users into its development has become more important in ongoing planning processes.

### **Conclusions**

Almost 10 years experience in applying information and communication technology to integrating and displaying data has shown it to be a key tool in trying to lessen uncertainties in maritime operations, in facilitating trade and in maritime security. The GRAFIMAR system gathers and integrates maritime data resulting in a useful and timely product for decision making processes. It might be possible in the future for this product to be made available to shipowners, forwarders, importers and exporters, in order to facilitate more effective management within maritime trade.

An important consideration in the success of the system is its reliance on the goodwill of private and public entities involved in maritime trade to work together for common objectives through the electronic exchange of information. Furthermore, the digital gap has diminished, which has allowed DIRECTEMAR to increase the system's operability and use of electronic methods to facilitate maritime trade. However, education and good planning have also been essential factors in facilitating these outcomes.

DIRECTEMAR now aims to make GRAFIMAR available to other economies so as to improve their C4ISR activities, and to contribute to one of the key objectives of APEC's STAR agenda – to facilitate a more secure trade environment.



# AVIATION SECURITY

## A3 – Karsof™ Total Airport Security System (Malaysia)

### Background

Malaysia has introduced the Karsof™ Total Airport Security System at Kuala Lumpur International Airport (KLIA). It uses biometrics technology based on fingerprints as the mode of identification and authentication for airport staff and visitors. A technology company specialising in software development and maintenance provided the system and related services.

### Objectives

The Karsof™ system aims to provide security and safety to airport users. It establishes a secure environment by identifying authorised visitors and allowing only those visitors and airport users such as staff and pass holders to enter restricted areas. It is an additional security enhancement to KLIA's current security system.

In addition to improving security, the system will support KLIA's stature as Malaysia's premier gateway and its aim to achieve a regional hub status. It will help KLIA implement ongoing improvements to meet national security objectives, and to promote state-of-the-art security infrastructure.

### Karsof™ Security System Structure

The Karsof™ Total Airport Security System is a specialised biometrics technology using fingerprints as the mode and basis of its biometrics identification and recognition technology. The technology is based on 'one to many' identification and recognition which verifies individual fingerprints from a large database of fingerprints. The system was developed specifically for KLIA to cater for approximately 27 000 pass holders and deals with 150 000 transactions per day. It is used by all airport staff and visitors.<sup>21</sup>

The system is based on the capture and recording of fingerprints, at least two for each person, during the enrolment process. Unique data is then extracted from the fingerprints and the system verifies the identity of a person by determining if the features extracted match the person's fingerprint (Figure A3).

The Karsof™ system undertakes the following tasks:

- ensures the security ID is valid;
- identifies the authorised airport staff and visitors seeking to access the secure area;
- analyses airport staff and visitor access in the airport;
- ensures the airport staff and visitors' access is authorised by the relevant security authorities;

21 The system is used by people in the following areas: fire station, airfield ground lighting, airside operation, airport operation centre, airside transit hotel, security and safety division, baggage handling system, contract and development, carpark management office, communication, commercial landside, directorate, electrical power system, finance division, flight operation centre, gas, head of division office, operation department, human resource department, infrastructure, legal, Malaysia airports properties, Masjid KLIA, business development division, general managers office, management services, operation services, technical group, technical services, customs, national security, police, immigration, airline staff and all government ministers and high officials.

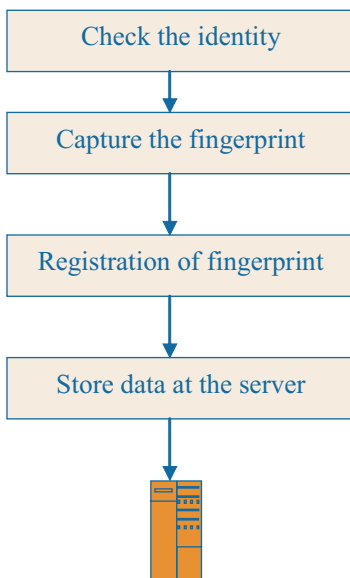
- ensures the security access device is in place at main security points; and
- ensures the correct identity of airport users, including some passengers, crews, visitors, staff and pass holders.<sup>22</sup>

The Karsof™ Total Airport Security System has the following unique features

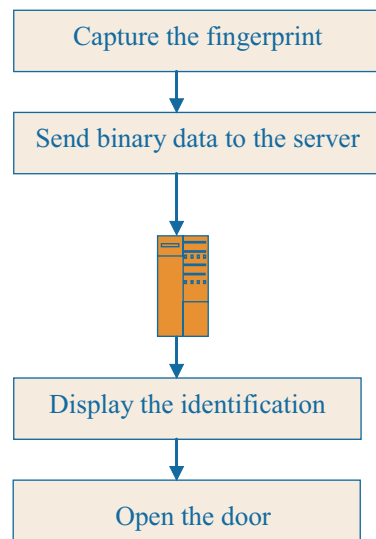
- integrated with existing sub-systems;
- the biometric technology uses a high performance identification algorithm which recognises, verifies and accesses data from any databases, regardless of their size, in about 0.5 seconds;
- fingerprint data storage enables a lowest fingerprint data storage size – less than 16 bytes (uncompressed) – the first of its kind in the world, compared to the industry standard of at least 256 bytes (compressed); and
- network security has a 1024 bit encryption level and public key infrastructure (PKI) with a unique dynamic protocol which switches the encryption level according to a change in protocol.

**Figure A3 Fingerprint Registration and Identification**

*Registration of Personnel Fingerprint*



*Identification of Personnel Fingerprint*



Source: Multimedia Glory Sdn Bhd Malaysia, 2004.

<sup>22</sup> Even though the actual enforcement for passengers is under approval, privileged passengers have used the system on a trial basis.

The security system includes an access control system, a time and attendance system and a daily pass system. The access control system places a biometric technology reader at entrances for staff or visitors, tracking airport staff or visitors' in and out transactions to and from secured areas. The time and attendance system is a biometric time clock for tracking airport operator employees' attendance.

The daily pass system enforces security access control at entrances with a biometric technology reader. The system identifies authorised visitors and allows only those visitors to enter restricted areas. Visitor access authorisation is guided by the built-in standard operating procedures (SOPs). The SOPs for visitors involved in the above systems are a pass request, pass approval, approval notification, pass issuance with fingerprint registration, access control enforcement based on the approval, pass return with financial penalties for any delay, system alert notifications to security, notification to enforcement agencies of any identification from a wanted database, background verification, and blacklist enforcements. The system also has built-in analysis reports providing statistical information on visitors using the airport.

### **Future Developments**

KLIA plans to enhance the biometric system. First, it will collaborate with databases such as immigration, criminal and police records (both domestic and international) and other relevant government agencies to vet personal backgrounds. It is envisaged that the vetting process will include passengers, crews, visitors, staff and pass holders. The vetting process will be online and will be done within seconds. Second, all security check points at the airport are to be made secure using the technology.

A possible future task is to implement the secure registration of passengers. This would require a centralised database. Passengers would be identified at the check-in counter or at the immigration exit. If a passenger was identified as a person of security concern, he/she would be stopped before boarding the plane. The admittance of passengers would be pending approval by the authorities.

### **Benefits Achieved**

Because biometrics uses a unique, measurable characteristic of a human being, it provides a very high level of security. It can be used for automatic recognition and for verifying identity quickly in real time. The Karsof™ biometric system:

- creates a secure environment at the airport by standardising security enforcement and by providing security to the entry and exit points of the airport by identifying authorised users and visitors and allowing only these to enter restricted areas;
- allows aviation security (AVSEC) personnel to more easily and accurately monitor and control staff and passenger movements and collects related statistics;
- provides passengers with a heightened sense of safety due to the visibility of security services;
- enables the identification of personnel using biometrics embedded with the automated SOPs; as a result, the entire system is streamlined and any identity misuse is detected and accordingly addressed with an automated alerting system with monitoring features;

- supports effective work plan management and enforcement;
- minimises the storage of millions of records on fingerprint data with identification time and verification unrelated to the size of the database;
- includes a biometric fingerprint test, which has been accepted by users as not overly intrusive, and which is convenient and simple to administer; and
- is designed through an open architecture so that it is able to collaborate on line with databases including immigration and police and criminal records, both local and international.

The local development of the technology specifically for KLIA enables the technology developer to fine tune, upgrade and enhance the software during implementation to provide optimum outcomes. Several general benefits arise from this. First, for KLIA, implementation of the technology improves its image. Also, local development of technology has led to increased knowledge and skills on biometric technology; particularly as a result of partnered systems development and transfer of technology programs.

### **Strategies to Deal With Risks/Obstacles Encountered**

For the biometric project at KLIA, much concerted effort was made to resolve problems to achieve the system's successful implementation. It required the appropriate order of implementation and support from technical and AVSEC personnel. In addition, it required a proper security plan covering all aspects of functional and operational system. A post-implementation review was also important to ensure the security objective had been met, and that it was properly implemented. All target groups were consulted in this process, including technical personnel, AVSEC and human resources personnel, the system developer/technology provider and airport users.

Implementing such a biometric system was also a broad managerial challenge for the airport authority. Management needed to ensure that the overall objectives of the project were aligned with the vision of the airport authority.

Problems that arose from the biometric system itself and from its operation and maintenance, included:

- change management problems, particularly as the technique was new and unfamiliar to staff;
- privacy concerns; addressed by the system being able to store a fingerprint in binary format rather than as an image;
- ensuring full enforcement; a necessity as any partial enforcement would undermine its effectiveness as a security measure; and
- integrating the SOPs with the biometrics security.

Before the system moved to the live environment, it underwent more than three months of testing, covering all pass holders and 13.5 million authentications. During the testing period, the service provider placed staff at every location to monitor



authentications (as well as from its central location). Daily log reports generated by the system were analysed by personnel to check that the system exhibited no false identification (false acceptance rate). The outcome of the testing period was that there were no false identifications.

## Lessons Learned

The primary goals in terms of implementing the Karsof Total Airport Security System were that it be robust and extendible, and have integrity, compatibility, efficiency, portability, ease of use and sustainability. Efforts in several areas helped to achieve these goals. An important part of this process has been for project managers to gain experience and incorporate 'lessons learnt' into project development and implementation.

### *Strong Planning*

The project's development and implementation was based on strong planning. Planning was primarily required to make everyone understand that no compromise resulting in a security breach would be acceptable. A system development plan was used to manage potential obstacles, which covered:

- user requirement analysis;
- strategies for customer acceptance;
- system development based on understanding of client and user requirements;
- adequate user training;
- attention to enforcement issues;
- post-implementation review; and
- possible need for fine tuning and future modifications/changes.

The last two items helped with developing newer versions of the system. The system development plan also included contingencies for failures in user acceptance, though these have not yet been required.

During the post-implementation review, solutions to overcome user difficulties were promptly developed. For example, the vastness of KLIA, and the remote locations of the system, caused operational problems for maintenance staff. This was addressed by implementing a centralised maintenance module that tracks the health of devices in remote locations so that staff are not required to physically monitor each location, thus improving the efficiency and effectiveness of the maintenance process.

As a result of the post-implementation review, features were also added to the system to enable staff to pre-emptively act to prevent an outage. This was an important enhancement given that the system is operated fully online without controllers, and any outage to the network would directly impact on its functionality.

A quicker response time to users' problems was also instituted. Communication between the user and the maintenance staff was streamlined through the user of instant messaging systems such as the short messaging system (SMS) and multimedia messaging service (MMS). User requests and problems are tracked at various levels, including through front level support, 2nd level support and the development team.

### *Stakeholder Interaction and Public-Private Cooperation*

The Karsof™ system relies heavily on data from external sources, which raised potential privacy and other issues. First, external sources did not always have the same understanding or objectives in relation to aviation security, necessitating an active role by KLIA in educating external sources about the important elements of aviation/airport security. The system is also linked with enforcement agencies for identification of criminals and wanted persons. To ensure data security for the enforcement agencies, their data is not extracted, but rather an extension server carries out fingerprint identification within their infrastructure. Data integrity for data used for personnel identification is achieved by verifying it in an automated process developed for the system. Apart from these measures, another key strategy in overcoming stakeholders' privacy concerns was the system is configured to read from the intermediate format in a way that is considered to take into account their privacy needs.

Airport management's role was critical in working with stakeholders to create an environment that facilitates technological change and organisational adaptation. This assisted in achieving greater acceptability for all users at KLIA. The top-down management approach involved management-level acceptance and fine tuning of the system based on user requirement and user acceptance. It was found that AVSEC/HR and technical personnel were able to obtain benefits from the system through its integration with the organisation's needs and, over time, with system development and enhancements.

In terms of conveying confidence to users and other stakeholders, the collaboration between AVSEC, human resources and technical personnel in supporting post-implementation of the technology, was essential. The post-implementation review improved user confidence levels in the system as it provided a guideline for enhancements. Successful user acceptance also required training sessions, and ample opportunity for their input, for example, through surveys.

### *Efficient Use of Technology*

One of the goals of the Total Airport Security system was ease of use so that airport efficiency would not be affected and would even improve. Using fingerprint identification with an easy-to-use reader ensures that this is the case.

The open source architecture used caters effectively for technology growth; providing flexibility and removing typical constraints inherent in other database or operating system architectures, which limits future business functionality. The system also interfaces with external systems due to its open architecture, for example, it is linked with enforcement agencies for online verification. Without such functionality, the SOPs would need to be modified to accommodate batch processing, which is not user-friendly.

With the sensitive nature of the security system, extra care has also been taken to protect data storage using innovative technologies such as the Karsof™ Business Continuity System. This enables the remote servers to be used as backup locations with their data updated immediately. The system also provides immediate fail-over to the backup servers during fatal disasters such as fire, ensuring smooth functioning of



business. Vandalism was also one of the main problems at KLIA. To address this, the devices were hardened to be resistant to the vandalism activity.

### *Education and Capacity Building*

The system provider gave specific training to KLIA personnel to operate the system and for its maintenance. Primary users were trained on the application in two four-hour sessions in the training room or on site. A comprehensive one day session for the system administrator was delivered prior to the user training to assist them in understanding the capabilities of the system. The system administrator also participated in the installation process, learning by working with the system provider's team. System documentation, including a users' guide, and a system guide was also developed to support users.

Training was successful, partly due to the following factors:

- training was in the local language;
- training was based on the SOPs being followed;
- any changes in the SOPs were identified and explained to trainees; and
- trial runs and on-hand training using mock environments were utilised.

A part of user education is the management challenge of changing the airport community's mindset when using the new system. This takes time and patience. The management tasks involved identification of user requirements and concerns, evaluation of the system to ensure it meets needs and objectives, and system enforcement.

### *Application to Other Economies*

It is the view of the provider that the Total Airport Security System could be implemented by other economies and that only minor modifications would be necessary to accommodate the SOPs specific to other regions/economies. Features of the system, such as user friendliness, flexibility and low implementation and infrastructure costs, could facilitate wide implementation; i.e. in other economies also. KLIA's experiences in addressing difficulties in adopting the system provide a strong learning curve for economies looking at implementing similar technologies.

## **Conclusions**

The major lesson learned from implementing the Karsof Total Airport Security System was that security must be enforced with user acceptance. Major factors contributing to the success of the system were management acceptance in the first instance, and flexibility in addressing user concerns and in making beneficial changes. Airport management also played a major role in the success of the system as a security tool. They were responsible for aligning KLIA policies with the system, and for enforcing its use.

The major lesson concerning sustainability and usability of the system, was that flexibility and adequate consultation processes are required. Based on the user problems identified in the post-implementation review, the system providers employed innovative solutions and methods to improve efficiency. Private-public interaction was also been important in its adoption and use, particularly interfacing with enforcement agencies. KLIA is now ready to use the Karsof Total Airport Security System with minor modifications.



# BUSINESS MOBILITY AND HUMAN SECURITY

## A4 – Australia’s Advance Passenger Processing System

### Background

Advance Passenger Processing (APP) is Australia’s version of an Advance Passenger Information (API) system. API systems provide government border agencies with advance notice of a passenger’s arrival on a particular flight or vessel (Department of Immigration and Multicultural Affairs, 2001). This initiative was developed in APEC’s Informal Experts’ Group on Business Mobility (IEGBM). Three APEC economies have already implemented API systems as of July 2004 – Australia (APP), New Zealand (Advance Passenger Screening system) and the United States (Advance Passenger Information System) – while a number of other economies have announced that they intend to do so as soon as practicable.

### Objectives

API systems improve security and also facilitate people movement. Australia’s APP system aims to prevent inadequately documented passengers from being uplifted by airlines overseas and to increase the efficiency of incoming passenger processing at airports, thus meeting STAR’s counter terrorism objectives and the requirements of the 2001 APEC Leaders’ Counter Terrorism Statement. API systems also contribute to APEC’s trade and investment facilitation agenda by enhancing the mobility of genuine business people, consistent with the business mobility goals of the Osaka Action Agenda.

### Australia’s APP System

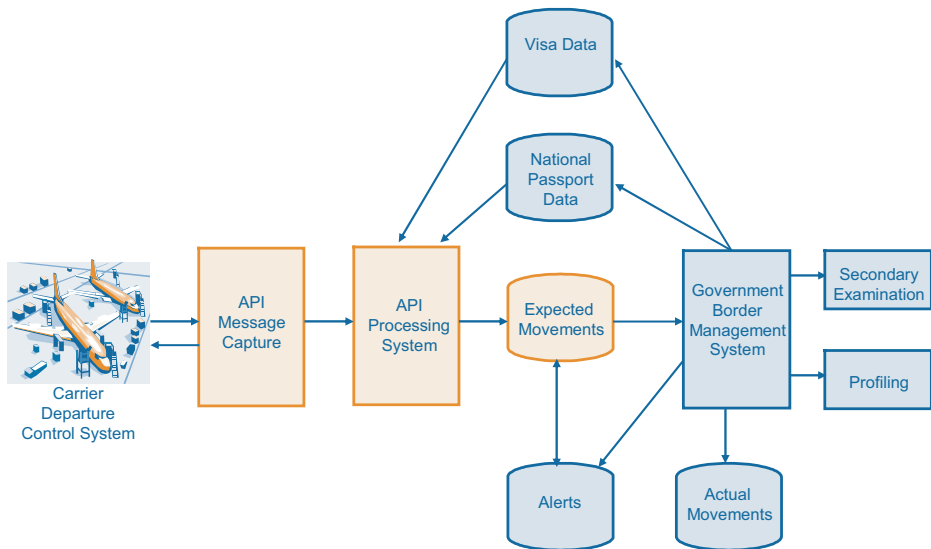
Australia’s APP system is based on a partnership between the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA), CPS Systems Pty Ltd and SITA.<sup>23</sup> The Australian APP system has been developed over the past 10 to 15 years as a totally integrated and interoperable Border Management System (BMS) providing airlines and Australian Customs Service (Customs) officials with a capacity to check the travel authority of all passengers in real time, at check-in and again at the border, and send advance passenger information to Australian border agencies via the global communication network provided by SITA. Using this network, airlines are able to access Australia’s APP system through specially developed interfaces within their own Departure Control System (DCS).

The system provides an individual record for each traveller on-line as he/she checks-in for the journey and an immediate boarding directive is provided to the

<sup>23</sup> SITA, originally called the Société Internationale de Télécommunications Aéronautiques, is an international association providing data and telecommunications services to the international airline industry ([www.sita.aero](http://www.sita.aero)). Australia’s border agencies are the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) and the Australian Customs Service (Customs). Two key responsibilities for DIMIA are to ensure that Australia’s immigration border controls are an effective barrier to the entry of persons who have no legal entitlement to enter Australia and to prevent the travel to Australia and entry of those whose presence in Australia is not in the public interest (DIMIA, 2003). In conjunction with the ACS, DIMIA provides an immigration clearance service to international passengers at Australia’s airports and seaports.

check-in agent based on the information held in the various databases. At the time the passenger checks-in for their flight, airline check-in staff enter the passenger's Australian or New Zealand passport number or Australian visa number into the APP screens in their DCS and this data is forwarded electronically to the Australian APP system hub where the system checks the passenger's details against departmental databases. APP then confirms the existence of a valid visa for those passengers requiring authority to enter Australia and the passport status of Australian and New Zealand travellers to ensure that the passenger has a valid Australian or New Zealand passport (Figure A4).<sup>24</sup> This assures Australian border agencies and the airline that the passenger is properly documented and authorised to travel to Australia.

**Figure A1 Schematic Diagram of Australia's APP System**



Source: Department of Immigration and Multicultural and Indigenous Affairs, 2004.

The APP checking process takes only a few seconds with confirmation of the authority to travel to Australia confirmed to the airline check-in staff in real time. If the passenger holds a valid visa or valid Australian or New Zealand passport, the check-in clerk receives an immediate 'OK to Board' message. If no immigration record is found for the passenger, a 'Do Not Board' response is provided and the passenger will not be permitted to travel until the matter is resolved. The APP system provides an Expected Movement Record (EMR) of the passenger to the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) which forwards this record to the Entry Control Point for validation when the passenger arrives in Australia. The EMR is also available for Australian authorities for further pre-arrival screening.

<sup>24</sup> New Zealand citizens travelling with a valid New Zealand passport are permitted to travel to Australia without a visa and are granted an entry visa on arrival at an Australian port.

Australia provides around-the-clock assistance to airlines who wish to resolve 'Not OK to Board' cases through a dedicated 24/7 Entry Operations Centre located in Canberra. Most boarding issues can be resolved in a matter of minutes. Passenger information collected at check-in is also forwarded electronically to Customs and other authorised users by DIMIA.

In January 2003, Australia made the collection and transmission of air passenger information using the APP system mandatory and, through 2003, both airlines and the cruise shipping industry rolled out APP incrementally. On 30 June 2003, some 97 per cent of air arrivals were covered by APP compared with around 65 per cent a year earlier. From 1 January 2004, all airlines travelling to Australia have been required to provide APP information on all passengers and crew and, in a significant enhancement to Australia's immigration screening process, for the first time international cruise ships have also been required to provide APP information in respect of passengers and crew. This ensures that all persons arriving in Australia from international passenger aircraft and international cruise ships are processed using the APP system.

The overall system is controlled and managed by DIMIA in accordance with Government IT best practise standards. DIMIA has developed Disaster Recovery and Business Continuity Plans for the system, in conjunction with CPS Systems Ltd, which meet current industry standards in terms of both disaster recovery and security.

### **Future Developments**

To cater for expected increases in passenger growth, border agencies, airlines and airport owners are working together to ensure that API systems continue to deliver tangible and measurable benefits (Australian Customs Service, 2004). In particular, DIMIA and Customs are working closely with international airlines to enhance the functionality and capacity of Australia's APP system to ensure that it meets the needs of both airlines and governments.

Customs is working on a program to access and evaluate information held in airline reservation systems which will provide a range of functions to enable it to determine in advance of a flight's arrival whether a passenger poses a potential risk to border security. A number of key international airlines are part of the program and Customs is working towards 100 per cent coverage (Australian Customs Service, 2003).

The widespread availability of international telecommunications systems infrastructure offers the potential to expand this technology across APEC (Business Mobility Group, 2004). APEC economies are working together to ensure that national API systems meet agreed standards while also meeting national border management goals. Standardisation of data elements and airline/government systems' interoperability provides the potential for further enhancement of identity checking by allowing confirmation of identity against information contained in biometric indicators and in each others' passport and other relevant databases (Informal Experts' Group on Business Mobility, 2003).

## Benefits

APP allows Customs and DIMIA to offer an unparalleled level of service delivery to passengers, airlines, airport operators and taxpayers. The APP system's advantages are that it:

- provides advance information on travellers arriving;
- screens out persons who do not have authority to travel to and enter Australia;
- confirms the existence of valid travel documentation;
- can be integrated into a departure system, ensuring that arrival and departure records are matched;
- requires only limited inputting of data at the check-in stage because data is already contained in secure Australian immigration databases;
- provides airline staff with fast and accurate responses; and
- can be configured to operate for both air and sea travellers.

From a counter terrorism viewpoint, the APP system ensures that persons who are not authorised to enter Australia are prevented from boarding flights and vessels bound for Australia. The APP system provides a highly effective 'real-time' immigration screen at the check-in counter overseas, allowing for early identification of persons of interest. Airlines' use of already existing telecommunications infrastructure to verify passengers' travel authority and then provide advance passenger information to border agencies has led to a quantifiable reduction in undocumented arrivals.

An important non-security benefit is that API systems reduce passenger processing times. Australia's experience has shown that processing times at airports can be approximately halved for APP-processed passengers. For both airlines and their passengers, APP means greater convenience both at the check-in point and when the passenger arrives in Australia. For government, it significantly improves border security and facilitates passenger clearance at international airports and seaports. For example, passengers can, if the economy so decides, be directed to receive faster clearance on arrival and departure through the use of 'express' lanes set up for API-processed passengers, particularly advantageous for frequent business travellers. This is possible because API-processed passengers have usually been 'pre-processed' by border control and immigration authorities prior to their arrival. The enhanced facilitation of passengers on arrival and departure, through pre-processed data, also ensures that passengers can check-in later and avoid long delays in border control. In addition, growth in passenger traffic can be managed without increased processing times through improved use of existing technology, rather than through the development of additional, and very costly, port infrastructure.

Other broader benefits of API or APP-type passenger processing systems include procedures and methods of data collection which aim for optimum data accuracy and more effective allocation of staff based on advance information on arriving or departing passengers. The opportunity to minimise costs through cooperation



also exists and improved communication and consultation between airlines and government allows for flexibility to accommodate airlines' individual needs.

These benefits should be able to duplicate in all economies using API or APP-type passenger processing systems. Implementation of these types of border management systems around the region will deliver seamless cross-border travel and significant savings for regional airlines and governments (Business Mobility Group, 2004).

### *Obstacles*

However, the disadvantages of the system are that:

- it can be expensive to implement, depending upon the current border management system in place;
- it requires a universal visa system (although not so for New Zealand or US systems);
- it needs to maintain centralised databases;
- it requires round the clock system availability and operations centre support; and
- it needs a dedicated communications network.

## **Lessons Learned**

### *Stakeholder Cooperation/Public-Private Sector Interaction*

DIMIA maintains close cooperation with key stakeholders, including all airlines flying into Australia, CPS Systems and SITA. By linking DIMIA databases with the SITA network, Australia has been able to use the well-established SITA network to check the authority of all passengers to enter Australia before travellers board their flights to Australia, without investing in additional infrastructure and keeping costs to a minimum.

Working closely with stakeholders using the system so that they have input to the system minimises disruption to their processes and ensures an efficient and effective outcome. Australia has worked closely with airlines over many years in the development and implementation of APP. The system has been developed incrementally as DIMIA's business requirements have changed. The development and maintenance of a cooperative relationship with airlines and other stakeholders has been a fundamental feature of the development and implementation of each phase of APP over the years. The day-to-day use of the system also relies on the support and input of international airlines. To ensure it operates effectively, Australia provides 24 hour assistance to airlines in resolving cases.

### *Regional Cooperation*

Recognising the gains to be made from the network effects of API systems and the benefits of interoperability, much effort has gone into setting standards. Australia has worked closely within APEC and other multilateral bodies and with other economies. Outside of APEC, Australia, the United States, Canada and the United Kingdom have shared technical information and have considered the need for standards to assist the

development of respective unilateral API systems. Specifically, these four countries have considered the need for minimum API data standards for border checks and technological standards to allow electronic exchange, confirmation of data and interactive document and alert checks.

Within APEC, economies have developed a comprehensive Statement of Principles to be adhered to as APEC members develop their own API systems.<sup>25</sup> The IEGBM found that to achieve standardised API systems across economies, a set of common API data elements was needed. It was agreed that a minimum set of data elements, common to all economies, should be developed with each economy having the capacity to add to the common set to meet its individual requirements. It was also agreed that future API systems should be developed to incorporate this flexibility. The IEGBM agreed on a common set of API data elements and other non-standard elements were also identified by individual economies to aid in system development. To ensure interoperability, the development of the full set of API data elements takes into account the IATA/WCO guidelines on API and the identified requirements of respective customs organisations.

### *Efficient Use of Technology*

The Australian APP system's use of the existing SITA network to link the airline reservation systems with DIMIA databases has ensured that Australia has been able to use already existing and proven technology to implement the objective of having all travellers checked prior to boarding. The process takes data already contained in the Machine Readable Zone (MRZ) of the traveller's passport to check the authority to travel. Australia requires airlines to collect only the data in the MRZ on the traveller passport and does not require any additional information to be collected by the airline. Airlines develop their own interface within their DCSs, thereby ensuring that their check-in clerks are presented with the best possible interface to the SITA network. DIMIA does not control the interface that each airline creates but works in partnership with CPS to ensure that the interface that is developed is compatible with both the SITA and the APP systems.

To ensure the highest level of effectiveness and efficiency, the development and implementation of global API systems and related standards underlies Australia's APP system. Australia has worked closely with other members of the International Air Transport Association (IATA) and APEC on technical issues relating to API systems. In particular, Australia has focussed on the need for standards to assist the development of respective unilateral API systems. IATA and the APEC economies considered the need for minimum API data standards necessary for border management authorities to undertake border checks as well as the technical standards for a common API data system that will allow electronic exchange and confirmation of passenger data along with interactive document and alert checks (Informal Experts Group on Business Mobility, 2003).

<sup>25</sup> The APEC Statement of Principles states that a 'standardised API system' should include the following key elements: be user-friendly, seamless and facilitate the travel of genuine passengers; take into account the needs of stakeholders, including other relevant control authorities; the UN EDIFACT messaging protocol is seen as a possible standard; the operation of an API system must be mindful of State policy and laws and any relevant international directives/agreements; where possible, leverage off existing industry infrastructure; be developed to be widely available and have the capacity to operate in a future bilateral/multilateral environment; have the capacity to provide 'Board/Do Not Board' directives; and include technological standards.

IATA agreed that a key element in achieving standardised unilateral API systems was to reach agreement on a set of common API data elements. As each economy had a different set of data requirements, IATA has worked to develop a minimum set of common API data elements to be collected as each economy develops its own API system, with each economy maintaining the capacity to add to the set to meet its individual requirements.<sup>26</sup>

By cooperating on technical issues, the use of API systems will increase and the savings will be magnified. As of August 2004 five APEC economies have implemented the API and a further thirteen have completed or are committed to completing feasibility studies. APEC's Informal Expert Working Group on Business Mobility also developed a set of technological standards for API systems.<sup>27</sup>

### *Strong Planning*

From the early stages, DIMIA managers have engaged key stakeholders and partners in all planning activities and key partners have been involved closely in developing systems specifications as well as implementation programs. DIMIA has carefully planned and managed every stage of the development of Australia's APP system in close partnership with private sector partners, including airline partners, SITA and international and national IT companies. The system provider, in particular works extremely closely with DIMIA staff to manage system change processes, from the earliest stages to system and user acceptance testing with airlines.

### *Applicability to Other Economies*

The implementation of API systems in other economies will add significantly to the long term technical capacity of border security and/or immigration authorities within APEC economies for expedited processing of passengers and the detection of unauthorised travellers. This is due to:

- increased intelligence and data collection opportunities;
- improved integrity of current immigration screening processes, which can be further enhanced by the capacity to link databases and share alerts;

---

26 The proposed API data elements were first developed by IATA's Control Authorities Working Group (CAWG) and adopted by IATA in 2003. The standards take account of the World Customs Organisation (WCO) guidelines on API systems development (Informal Experts' Group on Business Mobility, 2003). The IATA Statement of API Principles also adopted technical standards as minimum requirements for an effective API system. These include an automated system to reduce the amount of manual data entry at check-in; a system that is able to interface with other systems operated by governments and private sector agencies, eg. Passports; a system to provide for on line and real time communications between government and airlines' computing systems; to the extent possible, utilisation of existing government databases that contain passenger bio-data to avoid the need for manual data entry; the capacity to accommodate biometric information and images and to expand to meet anticipated growth in airline traffic; and a capability of ongoing 24 hourly operation with adequate fallback procedures to minimise disruption to airline operations in the event of system failure (Informal Experts' Group on Business Mobility, 2003).

27 The set of principles states that a standardised API system should meet the following technological standards: be automated and seek to reduce the amount of manual data entry at check-in; be able to interface with other systems operated by governments and private sector agencies (passports/visas); provide for on-line and real time communications between government and airlines' computing systems; to the extent possible, utilise existing government databases that contain passenger bio-data to avoid the need for manual data entry; have the capacity to accommodate biometric information and images and to expand to meet anticipated growth in airline traffic; be capable of 24/7 operation, with adequate fallback procedures to minimise disruption to airline operations in the event of system failure (contingency/disaster recovery plans).

- advance risk assessments; and
- the opportunity to enhance confirmation of identity via biometrics.

(Informal Experts' Group on Business Mobility, 2003).

The API data standards have been developed in such a way that they can be easily adopted by other economies. Economies can draw on their own experience to set their standards for the enhancement or development of a unilateral API system to meet their requirements, as their capacity enables them to do so (Informal Experts' Group on Business Mobility, 2003). Adoption of the API standards would provide economies with a comprehensive reference for the development of their own set of standards and the list can easily be added to by economies to reflect individual API requirements. Adopting the proposed data and technical standards could be expected to deliver the benefits of a standardised API process, such as improved passenger processing times, reduced number of undocumented passengers, minimised costs through cooperation, optimum data accuracy, and increased security and border control capabilities. These benefits are produced by increased intelligence and data collection opportunities, improved integrity of current immigration pre-screening processes (which can be further enhanced by the capacity to link databases and share alerts), advance risk assessments, and the opportunity to enhance confirmation of identity via biometrics.

Standardisation would ensure that the same benefits and capacities in respect of data collection, transmission and sharing are realised by all APEC economies joining the API environment. It would also ensure that newly developed API systems would be wholly compatible with the systems used by other stakeholders such as airlines. The standards would also allow for later enhancement so that economies may engage in passenger data and database sharing, subject to data security, privacy laws and other relevant legislation (Informal Experts' Group on Business Mobility, 2003).

## Conclusion

Through its experience with its APP system, Australia has found that such systems provide significant advantages, particularly in terms of improved border security and passenger processing times. The key issue driving success for a system which relies heavily on technology and information exchange has been regional cooperation, to ensure that systems are compatible and that the network benefits are maximised; this has involved agreeing and setting technical and informational standards. Another important factor in the successful implantation of the APP system was that costs were minimised by utilising existing networks and systems.

# FINANCIAL SECURITY

## A5 – Combating Money Laundering and Terrorist Financing – Indonesia’s Regime

### Background

Since 1999, Indonesia has worked toward establishing an effective anti-money laundering regime (AML) regime. The recent introduction of an AML regime and anti-terrorist financing (ATF) legislation makes significant progress towards correcting the defects in Indonesia’s criminal law and regulations. It upgrades Indonesia’s capacity to implement criminal law and regulation, and also strengthens cooperation in financial information exchange with overseas agencies.

### Objectives

An objective of Indonesia’s AML regime has been to provide for sanctions against money laundering to achieve both domestic and international aims of decreasing crimes relating to corruption and narcotics; increasing the integrity and credibility of the financial system; and meeting international commitments. This also reflects Indonesia’s commitment to halting terrorist financing. Related objectives have been for the AML regime to comply with the recommendations of the Financial Action Task Force’s (FATF), an intergovernmental body established in 1989; to accommodate public aspirations concerning financial security; and to be consistent with the development of the domestic legal infrastructure. ATF legislation complements the AML regime by criminalising the financing of terrorism.

### Regime Structure

Indonesia’s AML/ATF regime is underpinned by strong legislation.<sup>28</sup> The laws criminalise money laundering activities through 24 predicate offences.<sup>29</sup> The legislation also established Indonesia’s financial intelligence unit (FIU), as well as the Indonesian Financial Transaction Reports and Analysis Centre (or Pusat Pelaporan dan Analisis Transaksi Keuangan, PPAATK). It also places an obligation on financial services providers (FSPs) to submit suspicious transaction reports (STRs) and cash transaction reports (CTRs) to the PPAATK. Furthermore, the reporting, investigation, prosecution and justice for criminal offences of money laundering are exempted from the provisions of bank secrecy that are stipulated in the *Banking Law*. The money laundering law:

- has a reverse burden of proof in a court of law and the proceeds of crime can be frozen and confiscated;
- adds mutual legal assistance provisions so that Indonesian law enforcement officials may cooperate with foreign counterparts in the investigation and prosecution of criminal money laundering offences; and

28 The *Crime of Money Laundering Law Number 15 of 2002* as amended by the *Crime of Money Laundering Law Number 25 of 2003* and the *Criminal Acts of Terrorism Law Number 15 of 2003*.

29 These are corruption, bribery, smuggling of goods, smuggling of workers, smuggling of immigrants, banking offences, narcotics offences, psychotropic offences, slavery and trade in women and children, illegal trading in arms, kidnapping, terrorism, theft, embezzlement, fraud and other serious offences for which the proscribed penalty is four or more years in prison (the offence of terrorism is one of the new offences added) (APG Jurisdiction Report, Sept 2003) LS.

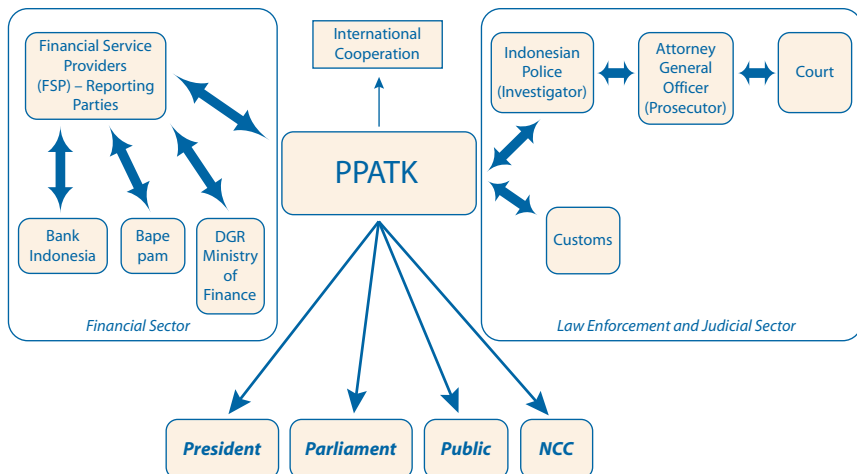
- enables the PPATK to take action on new identified developments in international conventions or recommendations.

The terrorism law also embodies the Indonesian government’s commitment to implement Article 3 of the UN Convention Against Terrorist Bombing (1997) and the UN Convention for the Suppression of the Financing of Terrorism (1999).<sup>30</sup> It criminalises the ‘financing of terrorism, the financing of the terrorist acts and the financing of terrorist organisations’ as described in the UN Convention. In addition, the law is the umbrella provision for other legislation relating to the eradication of criminal acts of terrorism. The law contains provisions relating to the financing of terrorist activities as criminal acts of terrorism, thus strengthening the AML regime. It also stipulates that competent authorities can freeze, seize and confiscate the proceeds of terrorism and assets used for terrorist activities. The AML laws require FSPs to make a STR when they suspect or have reasonable grounds to suspect that funds are linked to, related to, or are to be used for terrorism, terrorist acts or by terrorist organisations.

### How the Regime Works

The system comprises financial institutions and their regulators, law enforcement, the judicial sector and the government which interact to achieve the overall aims (Figure A5). Any person providing services in the financial field or other services in relation to finance is defined as an FSP and is covered by the regime.<sup>31</sup> Each FSP is required to submit STRs to identify transactions that deviate from the profile, characteristics and usual pattern of a customer’s transactions.

Figure A5 Indonesia’s AML Structure



Source: PPATK, 2004.

30 Indonesia has signed but has not ratified the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism, however Law No. 15 Year 2003 fully implements the convention.

31 These include, but are not limited to, banks, financial institutions, securities companies, mutual funds managers, custodians, trust agents, depository agencies, foreign exchange traders, pension funds, insurance companies and the post office.

The AML/ATF regime involves a number of regulators and supervisory bodies. Bank Indonesia, the central bank, as banking supervisor and regulator, has the power to license, prescribe regulation, and supervise and impose sanctions on the banking system. It supervises the implementation of AML policy, including the implementation of know your customer (KYC) principles in the banking sector.<sup>32</sup> Its objective is to ensure that banks are not being utilised as targets and/or mediums for money laundering activities. The Capital Market Supervisory Agency (BAPEPAM) guides, regulates and supervises the capital market to underpin fair and efficient capital market activities and to protect the interests of investors and the public. It also supervises the implementation of KYC principles in the capital markets. The Directorate General of Financial Institutions (DGFI) of the Ministry of Finance is responsible for supervising non-bank financial institutions, including providing licences and prescribing regulations, and supervises the implementation of KYC principles in these institutions. The AML/ATF laws and relevant regulations made by these bodies require financial institutions to collect information on the originator of fund transfers and retain information on the originator of fund transfers for five years.

The law enforcement and judicial sector involves the Indonesian National Police as investigator, the Attorney General's Office as prosecutor and the courts as adjudicator.

The PPATK is an independent agency responsible directly to the President of the Republic of Indonesia, which has the authority for preventing and eradicating the criminal offences of money laundering. It began operating in October 2003. Its duties are to:

- collect, maintain, analyse and evaluate information it obtains;
- monitor records in the exempt registry prepared by providers of financial services;
- prepare guidelines of procedures for reporting of suspicious financial transactions;
- provide advice and assistance to relevant authorities concerning information it obtains;
- issue guidelines and publications to providers of financial services concerning their obligations and assist in detecting suspicious customer behaviour;
- provide recommendations to the government concerning measures for the prevention and eradication of money laundering criminal acts;
- report the results of analysis of financial transactions indicating the existence of the crime of money laundering to the police and to the Public Prosecutor's office;
- provide reports regarding the results of analysis of financial transactions and other activities every six months to the President, the Parliament and to financial services regulators; and
- provide information to the public concerning its institutional performance.

---

<sup>32</sup> The three main financial regulators have released regulations setting out the KYC principles. The regulations include the obligation to stipulate policies and procedures for opening an account and for identifying the potential customer, for monitoring the customer's account and transactions and for risk management.

The PPATK requests and receives reports from FSPs and can grant exemptions from the reporting obligation for CTRs. It can request information concerning the progress of an investigation or prosecution of money laundering criminal acts. It also conducts audits of providers of financial services in respect of their compliance with the law. However, PPATK does not have investigative powers. Thus, PPATK is not an investigative unit; information is collected, processed and disseminated as required. The PPATK has issued six guidelines covering prevention and eradication of money laundering, identification of suspicious financial transactions, procedures for reporting of suspicious financial transactions, and cash transaction reports and reporting procedures.

The National Coordination Committee (NCC) is a ministerial-level body formed to ensure coordination and cooperation between ministries relevant to the fight against money laundering. It is responsible for coordinating the effort to prevent and eradicate the crime of money laundering; providing recommendations to the President; evaluating the implementation of the prevention and eradication of the crime of money laundering; and reporting on the progress of the prevention and eradication of the crime of money laundering to the President. It is assisted by a working group of high officials from relevant agencies. The working group may involve representatives of providers of financial services, experts, or other relevant parties in its discussions if necessary.

### **Future Developments**

PPATK currently receives most STRs and CTRs manually, but is planning for a switch to an almost entirely electronic submission system once the necessary computer infrastructure is in place. In addition, while analysis is currently done manually, it is expected that computerised analytical programs will be employed to assist the analysis effort. The availability of support software will make STR analysis significantly more effective. To ensure analysis is effective, specialised training in forensic accounting will be sought from economies that have the relevant expertise. This training should be in the form of long term placements of PPATK officers in actual working environments and the placement of forensic accounting mentors within PPATK.

### **Benefits Achieved**

The establishment of the ATF/AML regime is an important step in assisting Indonesia in its consideration for removal from the list of Non-Cooperative Countries and Territories (NCCT). Being on the list has raised the premium for Indonesians conducting transactions in international financial markets and has also increased costs of rebuilding the economy.<sup>33</sup>

### **Risks/Obstacles Encountered**

PPATK and other relevant agencies faced several problems and challenges in PPATK's first 12 months of operation when it was attempting to develop an effective AML/ATF regime in Indonesia. They found that there needed to be coordination among and cooperation between relevant agencies as well as with the private sector and the

---

<sup>33</sup> In June 2001, the FATF placed Indonesia (along with 19 other economies) on the NCCT list due to its absence of a money laundering law with criminal penalties, loopholes in financial regulation, inadequate resources for preventing, detecting and repressing money laundering activities, and the lack of international cooperation.

community to institute such a wide ranging regime. Also, increasing public awareness was found to be necessary as the AML/ATF regime was relatively new to Indonesia. In addition, as FSPs are the front guard in the regime, comprehensive regulations will need to be introduced to boost their compliance with reporting.

## Key Lessons Learned

### *Public-Private Interaction and Stakeholder Cooperation*

Stakeholder cooperation and interaction between public and private organisations was imperative to meeting the AML/ATF regime goals. The Government of Indonesia has done much to ensure that information can flow effectively between relevant bodies.

PPATK cooperates with other relevant domestic agencies, underpinned by memoranda of understanding, particularly in relation to financial intelligence, to ensure that information exchange occurs smoothly. These include Bank Indonesia, BAPEPAM, DGFI, the Directorate General of Tax, the Directorate General of Customs and Excise, the Indonesian National Police (POLRI) and the Centre for International Forestry Research.<sup>34</sup>

Indonesia established the NCC on anti-money laundering to enhance the strategic implementation and coordination of the AML/ATF regime. This ministerial level committee ensures coordination and cooperation between relevant ministries, such as Political and Security Affairs, Economy, Justice and Human Rights, Foreign Affairs, General Crime and Finance, along with various agencies such as Bank Indonesia, PPATK, BAPEPAM, POLRI, the National Intelligence Agency, the National Narcotics Agency and the Terrorism Eradication Coordination Desk.

Reporting guidance for FSPs is a crucial prerequisite for the smooth functioning of the PPATK. In order to ensure that FSPs understand the requirements placed on them, PPATK has issued guidelines to ensure FSPs comply with their reporting obligations. Other relevant authorities have issued regulations to ensure compliance with the KYC principle.

The Government of Indonesia made a concerted effort to include FSPs early on in the development of the AML regime. As early as 1999, the Indonesian Government, with assistance from Australian and US aid agencies – AusAID and USAID – was holding seminars with FSPs around the country to discuss the requirements of an AML regime. In these seminars, Indonesian officials and foreign experts explained the requirements that FSPs would need to meet if the Indonesian AML regime was to be successful. A major concern of FSPs at the seminars was that an AML regime would be expensive and drive away customers concerned with the privacy of their financial transactions. However, at the end of the seminars, the government along with their foreign colleagues had made some headway in convincing FSPs that not implementing an AML regime would ultimately have higher costs for them and their customers than implementing them would.

---

<sup>34</sup> One of Indonesia's main crime concerns is illegal logging of forest timbers, thus one of the crimes listed under Article 2 of the Law No. 25 Year 2003 is 'in the forestry field'.

### *Efficient Use of Technology*

It is PPATK's aim to facilitate low cost, efficient reporting mechanisms, which will save both the FSPs and PPATK considerable time and money in implementing the reporting regime. In achieving this objective, PPATK will involve the FSPs through consultation processes when developing and implementing its reporting regime. Information technology is becoming an essential part of the business to make an FIU fully operational in terms of receiving reports, analysing them and disseminating information to its partner agencies.

External assistance has played a significant role in enabling PPATK to adopt efficient technology to support the AML regime. So far, this includes initial office automation, line communications and a standard database. The initial outlay was provided by Bank Indonesia. USAID also assisted PPATK by providing initial IT hardware (US\$250 000 before tax). Further discussions are underway between PPATK, AusAID and the Australian Transaction Reports and Analysis Centre (AUSTRAC), to assist PPATK to develop some system modules. Nevertheless, PPATK is facing difficulties in procuring additional IT, due to time relays relating to government procurement guidelines.

### *Education and Capacity Building*

Financial investigation and reporting is a specialised area, thus PPATK considers that training is required to build, develop and increase the capacity and effectiveness of its personnel. It did this successfully through utilising international expertise. To improve PPATK capacity, around 57 PPATK personnel have been assisted by:

- an Australian Agency for International Development (AusAID) technical advisor with the start up management of PPATK;
- a United States Agency for International Development (USAID)/Economic Law, Institutional and Professional Strengthening (ELIPS) legal advisor with the legal and regulatory area;
- Australian Transaction Reports & Analysis Centre (AUSTRAC) technical advisors in the areas of STR analysis, law enforcement liaison, the international stream and the regulatory and compliance stream;
- the Asia Development Bank (ADB) Technical Assistance Project run by Deloitte Touche Tohmatsu, which worked on developing required guidelines, ensuring practical implementation of CTR, establishing effective and consistent supervision, compliance framework and a training program; and
- European Commission technical advisors with IT development.

This training meant that difficulties in applying the FATF, UN and other guidelines to the Indonesian financial services and legal environment were minimised.

A lingering problem is that the system makes it difficult to get suitable funding for independent bodies like the PPATK and, related to this, problems have arisen in providing suitable compensation to the staff. These issues are still being addressed.



### *Strong Planning*

Planning was essential in establishing a completely new regulatory structure and way of doing business. This has also involved educating the public. A lot of credit is due to the PPATK and those who worked on introducing the AML regime in the government before the PPATK was established. In addition, the donor community played an important role in the planning process. Working closely with the Department of Justice, AusAID cooperated early on with officials from the Indonesian Government and the donor community to talk about needs and to plan ways in which to meet them early in the process. This was a very well coordinated and cooperative development effort.

Planning is also required to make everyone understand that no compromise on compliance with the regime and on accuracy of reports will be acceptable. PPATK is taking care to ensure that the right procedures are being set up within the organisation to receive, process, evaluate and disseminate the reports, with associated financial data where it exists, in an effective and timely manner.

### *International Cooperation*

Because money laundering is a transnational, as well as a national crime, to eradicate it, the Government of Indonesia engaged in international cooperation through bilateral and multilateral forums. Indonesia realises the importance of international recommendations and best practices; the recommendations have served as essential elements in preparing policies for the prevention and eradication of the criminal offence of money laundering in Indonesia.

In order to enhance Indonesia's capacity to undertake the international exchange of financial intelligence, PPATK sought memoranda of understanding (MoUs) with 16 FIUs from other jurisdictions throughout 2003. PPATK has MoUs with partner agencies in Thailand, Malaysia, the Republic of Korea and Australia and has entered into an exchange of letters enabling information exchange with Hong Kong. Since 2000, Indonesia has been a member of the Asia/Pacific Group on Money Laundering (APG)<sup>35</sup> and it joined as a member of the Egmont Group in 2004.<sup>36</sup> Furthermore, Indonesia has fully implemented UN Security Council Resolutions involving terrorist financing.<sup>37</sup>

35 The purpose of the APG is to facilitate the adoption, implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations and Eight Special Recommendations on Terrorist Financing of the FATF. This includes assisting jurisdictions in the region to enact laws criminalising the laundering of the proceeds of crime and dealing also with mutual legal assistance, confiscation, forfeiture and extradition. It also includes the provision of guidance in setting up systems for reporting and investigating suspicious transactions and helping in the establishment of FIUs ([www.apgml.org](http://www.apgml.org), accessed 7 July 2004).

36 In 1995, recognising the benefits inherent in the development of an FIU network, a group of FIUs met at the Egmont Arenberg Palace in Brussels and decided to establish an informal group for the stimulation of international cooperation. Known as the Egmont Group, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise. There are currently 84 countries with recognised operational FIU units, with others in various stages of development. Countries must go through a formal procedure established by the Egmont Group in order to be recognised as meeting the Egmont Definition of an FIU ([www.egmontgroup.org/about\\_egmont.pdf](http://www.egmontgroup.org/about_egmont.pdf), accessed 7 July 2004).

37 S/RES/1267 (1999) Measures against the Taliban, S/RES/1333(2000) Measures against the Taliban, S/RES/1373 (2001) International Cooperation to Combat Threats to International Peace and Security Caused by Terrorist Acts and S/RES/1390 (2002) Measures Against Al-Qaida and the Taliban.

In addition, technical assistance coordination meetings between the PPATK and donors are held regularly, at least three times per year, and have provided positive benefits for the development of the AML regime in Indonesia. They discuss technical assistance needs for Indonesia's AML regime development, provide a priority list and are used as a forum to exchange information.

#### *Applicability to Other Economies*

Indonesia did not face unique difficulties in introducing its AML/ATF regime, and therefore its experiences are applicable to other (particularly developing) economies. Based on this case study, the primary factor a developing economy may need to take into account in implementing a similar regime is 'time' in light of competing priorities. Indonesia had been undergoing a transition to a democracy and the AML had to compete with a number of other reform needs. It did not therefore have the resources to give to AML that other, especially developed, economies have had. This slowed down implementation. Each economy would need to factor in its own unique set of domestic considerations into planning processes.

#### **Conclusion**

The activities of the Government of Indonesia show that it is serious about achieving an effective AML/ATF regime. It has made tremendous progress towards addressing weaknesses in its legal framework including developing an operational capability to enforce the new AML/ATF regime. The regime is correcting the defects in Indonesia's criminal law and regulations, upgrading Indonesia's capacity to implement them and strengthening cooperation in financial exchange with overseas agencies. Although Indonesia remains on the NCCT list, it is encouraged by the positive recognition of progress achieved and, with continued effort, Indonesia is hopeful of achieving an internationally recognised standard for AML within an appropriate and reasonable timeframe.

Indonesia has found that the key to implementing an effective regime is to take advantage of assistance from the international community, both in terms of developing the structure and processes of the regime, and in terms of training and capacity building for the relevant organisations. Good planning and strong internal consultation and coordination processes were also found to be integral aspects to effective implementation of AML.







