



**Homeland
Security**

The following document was received by the DHS Privacy Office.

For more information please visit the website at www.dhs.gov/privacy.

Additional Contact Information:

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Telephone: 571.227.3813
Fax: 571.227.4171
Email: privacy@dhs.gov



Asia-Pacific
Economic Cooperation

2006/SOM3/BMG/004rev1

Agenda Item: 5

Multilateral Framework for Regional Movement Alert System (RMAL)

Purpose: Consideration

Submitted by: New Zealand and Legal Experts' Working Group



**Business Mobility Group Meeting
Hoi An, Viet Nam
6 September 2006**

To: Business Mobility Group

Multilateral Framework for Regional Movement Alert System (RMAL)

Purpose

1. The purpose of this paper is to recommend that the Business Mobility Group endorse the attached Multilateral Framework (MLF) which will be the basis for APEC economies to participate in the Regional Movement Alert System (RMAL) for detecting and preventing the use of lost, stolen and invalid passports for travel and entry.

Mandate for Concluding a Multilateral Framework

2. This recommended final step in concluding an MLF fulfils the direction of earlier BMG Senior Officials Meetings on 8 September 2005 and 8 May 2006, supported by TLF funding from Japan for the Experts Working Group (Expert Group).

3. The content and direction of earlier drafting work was endorsed by BMG, enabling the Expert Group to continue its deliberations after its third workshop in Hong Kong 2-5 May 2006. At that stage, the group consisted of Australia, Hong Kong (China), New Zealand and USA experts who cooperated successfully to carry on with earlier contributions by Korea, Mexico and the Philippines.

4. Comments about the documentation tabled at SOM II on 24 May 2006 in Hanoi were received subsequently from Australia, Chinese Taipei, Hong Kong (China), Mexico, New Zealand, Singapore, and USA, and were taken into account by the Experts Group in finalising the MLF

5. In showing their confidence in the feasibility and acceptability of the attached MLF documents, senior officials from Australia, Hong Kong (China) New Zealand and USA have authorised their respective Expert Group officials to recommend endorsement of this MLF by the BMG.

The RMAL System

6. In concluding the attached MLF, the Expert Group has been guided by the RMAL System Guiding Principles and has applied the component parts of the RMAL System which consist of :-

- i. electronic records maintained by each participating economy of specified data elements of their lost stolen or otherwise invalid passports which are accessible in real time;
- ii. the automatic electronic checking of specified data elements of passports presented by persons as a part of intended international travel against the electronic records of specified data elements maintained by the participating economies;
- iii. the processes for registering and giving notice when matches of specified data elements ('RMAL hits') occur;
- iv. the maintenance and operation by each participating economy of a facility which is staffed continuously (24/7 facility) and available to verify RMAL hits in real time;
- v. processes by which participating economies manage the consequences, as determined by each participating economy, of RMAL hits.

7. The scope of the RMAL System activity covers the making available of the non-personal data elements, matching and checking the data, and personal information provision associated with the verification and consequences of 'hits'.

8. BMG has determined that the RMAL System should initially check for lost and stolen passports and that, in line with the RMAL System Guiding Principles, it should be interoperable with the existing border management systems or other regional or multilateral systems of enhancing border security, and operate seamlessly with the departure control systems. This principle does not assume a specific APP linkage.

Composition of MLF

9. The recommended MLF consists of several components, including a document of common principles and standards, a governance charter, and a model MOU, which are intended to deliver the RMAL System consistently and effectively for participating APEC economies. All components of the MLF should be read and applied together as each component has its particular purpose and reinforces the other two. The attached MLF comprises the following suite of documents:-

(i) **The Multilateral Framework (pages 6-13)** – establishes the common principles, standards and basic requirements that will guide the arrangements, governance and operations of the RMAL System in accordance with the principles the APEC Leaders have agreed.

The MLF has maintained all of the provisions reported to SOM II on 24 May 2006. The document provides an overarching principled framework for the two Annexes (the Management Board Governance Charter and the Economy Model MOU). [The Expert Group proposes the MLF as an effective and detailed statement of principles, standards and accountabilities which RMAL System participants should expect of each other in order to achieve effective consistency, accuracy and integrity of the RMAL System.]

(ii) **Annex 1 - The Management Board Governance Charter (pages 14-16)** - establishes the principles, responsibilities and processes of the Management Board for establishing and ensuring the necessary and continued governance, operational protocols and standards between participating economies.

The Management Board will provide strategic governance of the RMAL System. The Charter has been drafted by the Expert Group in relatively succinct, high level terms so as to enable the Board (once it is established) to develop its role and responsibilities in greater detail to reflect the dynamic operating environment of the RMAL System.

The Charter does specify the responsibilities, processes and activities of the Management Board. Among other things, the Board will be responsible for facilitating new RMAL System participants, agreeing funding arrangements, and overseeing any future development from its current scope and purpose concerning lost and stolen passports. It is proposed that the Board will be established immediately upon agreement by the BMG.

(iii) **Annex 2 - The Model Economy Memorandum of Understanding (Model MOU) (pages 17-24)** – establishes the conditions under which the participants may choose to make available to each other and support certain information on lost and stolen passports within the RMAL System, without affecting the essential sovereign authority of each participant to determine who is to enter its territory.

The Model MOU supports the MLF by enabling participants in the RMAL System to agree amongst themselves to the conditions for making information available to each other. The Model MOU reinforces the status of domestic law, and in effect, 'triggers' or activates the information provision between participants.

Although, by its very nature, the Model MOU is an agreement between individual economies, the Expert Group proposes that it be applied consistently with, so as to reinforce, the other parts of the MLF. A Senior Administrator from each economy will be named as the point of responsibility for ensuring the operation of the RMAL System consistent with the MLF, and the Management Board will be able to monitor arrangements because it will receive MOUs and any proposed amendments as between participants.

Because some flexibility in the operational arrangements between economies will be necessary, some operational aspects of the Model MOU have been segmented in an Annex called "Permissible Actions," which can be amended mutually by Senior Administrators without the complexity of amending the MOU itself.

[10. Participants will document and agree their respective standard operating procedures and technology requirements based on specific business process needs.

Key Points of Guidance

11. The Expert Group brings these particular points to the attention of BMG economies:-

(i) The RMAL System Pilot, with Australia, New Zealand and the USA, has successfully proven its security and facilitation value.

(ii) Previously identified gaps in the MLF relating to governance, accountabilities, administrative clauses, scope of the RMAL System, notification of hits before taking adverse action, records retention, review of data, disputes resolution, and the APEC Privacy Framework alignment, have been addressed in the attached documents.

(iii) A comparison carried out by the Expert Group has confirmed that a good level of consistency exists between the attached MLF documentation and the APEC Privacy Framework.

(iv) It should be noted that the MLF is not governed by international law and does not create legal obligations. To provide and receive lost and stolen passport data within the RMAL System, participating economies are expected to enter into MOUs with other participating economies.

(v) The work carried out in the pilot project by Australia, New Zealand and USA has delivered a lot of the detailed operational and technical specifications that support the RMAL System. This detailed documentation can be made available to assist aspiring participant economies in developing their readiness and capacity to seek entry to the RMAL System through the Management Board.

(vi) The establishment of the Management Board will be an important and immediate next step after endorsement of the MLF, in order to facilitate necessary governance of the RMAL System in production mode and the consideration of new participants.

Recommendation

12. It is recommended that BMG :-

Agree to the attached Multilateral Framework for the RMAL System including its supporting

Annex 1 - Management Board Governance Charter; and

Annex 2 - Model Economy MOU.

Brendan Quirk

New Zealand

(Chair, on behalf of the Expert Group members)

**MULTILATERAL FRAMEWORK
FOR REGIONAL MOVEMENT ALERT SYSTEM
(RMAL SYSTEM)**

Version Dated 31.8.06

**MULTILATERAL FRAMEWORK FOR THE PROVISION AND USE OF LOST,
STOLEN AND OTHERWISE INVALID PASSPORT INFORMATION AS PART OF A
REGIONAL MOVEMENT ALERT (RMAL) SYSTEM**

PREAMBLE

1. Terrorism and other trans-national criminal activity pose a major threat to national security and to economic prosperity throughout the world, including in the Asia-Pacific region. At the same time, the safe and efficient movement of legitimate travellers across borders is vital to the continued growth of trade in goods and services across the APEC region. As a result, APEC members acknowledge the need to manage effectively the movement of people across borders.
2. APEC leaders recognise that one way of enhancing the movement of legitimate travellers while preventing the movement of illegitimate travellers across borders is to co-operate and collaborate in the disclosure and use of information they collectively hold concerning the documents used by and other information about intending travellers.

RMAL GUIDING PRINCIPLES

3. APEC Leaders have, therefore, directed that arrangements be developed between their economies for the provision and use of such information in the form of a regional movement alert (RMAL) system in accordance with the following agreed principles:
 - (a) The scope of the RMAL System and its data should focus on enhancing counter-terrorism capacities of participating economies;
 - (b) The RMAL System design and operation will not affect the essential right of a participating economy to determine who is permitted to enter the economy and on what basis they are permitted to enter;
 - (c) Ownership and visibility of shared alert data would be vested in the economy that has provided that data;
 - (d) Participating economies should not be able to use the RMAL System to monitor nationals of other participating economies without the express permission of that economy.
 - (e) Privacy laws of each participating economy will be satisfied;
 - (f) The operating system could be built and deployed so that it operates seamlessly with the departure control systems of airlines flying to participating economies;
 - (g) The operating system would be built and deployed so that it complements and, if possible, is interoperable with, the existing border management systems of participating economies or other regional or multilateral systems developed for purposes of enhancing border security;
 - (h) Ultimately travel should be able to be monitored on a real-time rather than ex-post basis.

PURPOSE

4. The purpose of this Framework document is to establish the common principles and standards that will guide the arrangements, governance and operation of the RMAL System in accordance with the principles the APEC leaders have agreed. It does this initially by providing a framework for participating economies to provide each other information concerning lost, stolen and otherwise invalid passports in order to;
 - (a) assist in assessing the *bona fides* of prospective incoming passengers and facilitate travel of genuine passengers;
 - (b) assist participating APEC economies in efforts to counter terrorism, and other serious criminal activity;
 - (c) detect and prevent the misuse of lost, stolen and otherwise invalid passports;
 - (d) in accordance with the relevant ICAO Code of Conduct for Immigration Liaison Officers, and IATA Guidelines for the Removal of Inadmissible Passengers, remove lost, stolen and otherwise invalid passports from circulation.

SCOPE OF THE RMAL SYSTEM

5. The RMAL System consists of the following component parts:
 - (a) electronic records maintained by each participating economy of specified data elements of their lost stolen or otherwise invalid passports which are accessible in real time;
 - (b) the automatic electronic checking of the specified data elements of passports presented by persons as a part of intended international travel against the electronic records of the specified data elements maintained by the participating economies;
 - (c) the processes for registering and giving notice when matches of the specified data elements ('RMAL hits') occur;
 - (d) the maintenance and operation by each participating economy of a facility which is staffed continuously (24/7 facility) and available to verify RMAL hits in real time;
 - (e) processes by which participating economies manage the consequences, as determined by each participating economy, of RMAL hits.

6. The following key documents support the RMAL System;
 - (a) The Multilateral Framework including the Summary of Basic Requirements attached as Appendix 1;
 - (b) Management Board Governance Charter (attached as Annex 1);
 - (c) The Model Economy Memorandum of Understanding (MOU) (attached as Annex 2);

and the following documents established by each participating economy :-

- (d) Standard Operating Procedures;
- (e) Technical Specifications;

7. In the interests of consistency it is expected that economies' MOU's will follow the model form (which will set out the essential requirements for participation in the RMAL System) and be available to all participating economies.
8. The Multilateral Framework including Management Board Governance Charter and Model Economy MOU are to be publicly available.

GOVERNANCE AND ACCOUNTABILITIES

9. A Management Board comprising RMAL participants will be responsible for strategic and operational governance of the RMAL System.
10. In exercising its responsibilities as described in the Management Board Governance Charter, the Management Board will;
 - (a) be guided by the Multilateral Framework;
 - (b) ensure that the RMAL System provides the authorities of participating economies with information that is both timely and accurate and serves the RMAL purposes;
 - (c) set clear standards through which the operation of RMAL System can be measured;
 - (d) establish appropriate accountabilities and reporting mechanisms to ensure participating economies meet the standards necessary for the RMAL System's operation; and
 - (e) report to the BMG annually or as otherwise requested.

PARTICIPATION AND OPERATIONAL ARRANGEMENTS

11. Participation in the RMAL System is open to all of the APEC economies, provided that they meet the necessary standards and functional and operational requirements as set out in the key documents and provided that they enter into an MOU for disclosure and use of information with another participating economy.
12. Participating economies are encouraged to disclose information to the other participating economies. Provided they enter into a MOU with at least one other economy, each participating economy retains the discretion to determine whether or not it will provide information to any other participating economy.
13. The Summary of Basic Requirements for the operation of the RMAL System are summarised in Appendix 1 of the MLF document.

PRINCIPLES FOR MANAGEMENT OF INFORMATION

General principles for management of personal Information should be guided by the APEC Privacy Framework of 2004.

Quality of Information

14. Participating economies should take all reasonable steps to ensure the high quality and integrity of information provided and used in the RMAL System.

Use and Further Provision of Information by Requesting Economy

15. Provision and use of information in the RMAL System should only occur for the purposes of the RMAL System in accordance with MOU's between the participating economies.
16. If domestic laws require further use or disclosure of information for a purpose other than the RMAL System, the further use or disclosure should occur in a manner transparent to the relevant participating economies.

Security of Information

17. All information provided and used in the operation of the RMAL System should be handled in a secure manner and by persons suitably trained in the constraints of its use and disclosure.

Retention of Information

18. Retention of data and information should be based on the need to fulfil the purposes of the RMAL System and on continued participation in RMAL, subject to domestic legal requirements.
19. The RMAL broker will retain no information other than transaction identification numbers and transaction timing information.

Individual access to information

20. An individual's access to their personal information is to be determined in accordance with the domestic laws of participating economies.

Notice

21. Participating economies should take such steps as they consider appropriate to inform their public about the operation of the RMAL System and its implications for them.
22. Participating economies should take reasonable and lawful steps to prevent persons travelling on their own passports that they know are lost, stolen or otherwise invalid.

INFORMATION MANAGEMENT ACCOUNTABILITIES*Records Review*

23. Records should be kept by each participating economy to enable review of the performance and integrity of the RMAL information.

Response to Breach of Information Management Obligations

24. Each participating economy should provide mechanisms to address activity that undermines the integrity or security of information.
25. Participating economies may provide for appropriate responses in the event they determine an unacceptable risk exists to the integrity or security of RMAL data and information.

FINANCIAL ARRANGEMENTS

26. Financial arrangements will be agreed between participating economies through the Management Board.

DISPUTES RESOLUTION

27. Participating economies should identify issues that arise between them and use best endeavours to resolve them.

STATUS OF MULTILATERAL FRAMEWORK

28. This Framework is not governed by international law and does not create any legal obligations.
29. The provisions of this Framework should not prevent any participating economy from granting assistance in accordance with the provisions of other applicable international treaties, agreements or arrangements, such as the Convention on International Civil Aviation.
30. Nothing in this Framework supersedes the obligations of participating economies to report lost and stolen passports to the Interpol data base of lost and stolen travel documents by the end 2006 as detailed in the Joint Ministerial Statement of 16 November 2005 and endorsed by the leaders in the Busan Declaration of 19 November 2005.

DEFINITIONS

RMAL broker – means the centralised messaging mechanism that will provide security protection and pass messages between participating economies.

specified data elements – comprise the following:

- (a) passport identification number
- (b) issuing authority
- (c) type of document
- (d) date of issuance

24/7 facility – a facility maintained by a participating economy that is staffed continuously and available to support that economy's RMAL System and respond to inquiries from other participating economies in relation to RMAL hits.

otherwise Invalid - includes passports that have been revoked or recalled by a participating economy

passport – means any issued travel document that is lost, stolen, or otherwise invalid and any lost or stolen blank travel document.

participating economy – an APEC economy that has met the necessary standards and functional and operational requirements as set out in the key documents, has entered into a MOU for provision and use of information with another participating economy and is implementing that MOU.

information – means the specified data elements and such other information as may be necessary to appropriately respond to an RMAL hit.

**SUMMARY OF BASIC REQUIREMENTS FOR THE
OPERATION OF THE RMAL SYSTEM**

1. The RMAL System is a mechanism whereby the use of lost, stolen and/or otherwise invalid travel documents can be detected. This is done by directly accessing the document issuing authority's data in real-time to check whether or not a travel document is of concern.
2. A key objective of the RMAL System is to ensure that this checking occurs without disruption to travellers. It is therefore critical that the technological processes support the business objectives.
3. The RMAL System and its operation is to be based on a network of arrangements among the participating economies. It is expected that these arrangements will take the form of written agreements or Memoranda of Understanding (MOU) providing for the accessing of data elements of lost, stolen and/or invalid travel documents, together with supporting operational and technical arrangements.
4. The technical infrastructure consists of communication links between document issuing authorities, border agencies and a centralised messaging system ('Broker'). The broker is like a switchboard for routing queries and answers to and from border systems and the passport databases of participating economies. No data is stored in the broker.
5. Underpinning the technical infrastructure are a range of business processes and legal requirements, that at a minimum should include:
 - (a) Participating economies having a database of lost, stolen and/or otherwise invalid travel documents that can be accessed in real-time.
 - (b) Domestic legal authorisation enabling the accessing of data to reflect APEC and any domestic requirements.
 - (c) Operational support to enable investigation and resolution of RMAL notifications provided by a 24/7 facility, allowing consequence management to be facilitated in real-time by each economy.
 - (d) Mutually agreed upon standard operating procedures regarding the consequence management of RMAL notifications.
6. The Management Board for RMAL will coordinate the operational arrangements to ensure the integrity of the RMAL System.

ANNEX 1

**MANAGEMENT BOARD GOVERNANCE CHARTER
(REGIONAL MOVEMENT ALERT SYSTEM)**

MANAGEMENT BOARD GOVERNANCE CHARTER FOR RMAL SYSTEM

Introduction

1. The feasibility study report to the Senior Officials on 27 September 2004 in Santiago, Chile, suggested a Management Board composed of representatives of participating economies be created under the auspices of the Business Mobility Group (BMG) to manage the RMAL programme.

2. This Charter contains the principles, responsibilities and processes of the Management Board.

Principles for Governance

3. A Management Board, comprising RMAL participants will be responsible for strategic and operational governance of the RMAL System.

4. In exercising their responsibilities as described in this Management Board Governance Charter, the Management Board will

- (i) Be guided by the Multilateral Framework;
- (ii) Ensure that the RMAL System provides the authorities of participating economies with information that is both timely and accurate and serves the RMAL purposes;
- (iii) Set clear standards through which the operation of the RMAL System can be measured;
- (iv) Establish appropriate accountabilities and reporting mechanisms to ensure participating economies meet the standards necessary for RMAL's operation; and
- (v) Report to the APEC Business Mobility Group (BMG) annually or as otherwise requested by BMG.

Management Board Responsibilities

5. The Management Board will provide strategic governance of the RMAL programme consistent with the RMAL Guiding Principles and Multilateral Framework, and having regard to domestic legal obligations of each RMAL participant, including, but not limited to,

- a. the setting of operational protocols and standards in relation to:
 - programme oversight, including establishing accountabilities and supporting arrangements
 - administration and the necessary resources to support the Management Board
 - operations
 - technical guidance

- systems security/safeguards
 - conditions of use
- b. the establishment of a framework for participation
 - c. the funding arrangements
 - d. the future direction and development
 - e. dispute resolution.

Processes and Activities

6. The RMAL participants will maintain a Management Board comprised of one representative from each participating RMAL economy. The APEC host economy may provide a non-voting ex-officio representative.
7. The Management Board will appoint a Chair.
8. The Management Board will convene general meetings twice a year. Other meetings may be convened as needs of the program dictate and the Management Board may invite economies or other parties to participate.
9. The general Management Board meetings will be held in open forum and any economy is welcome to participate as an observer.
10. Any economy may submit topics for Management Board discussion at any time to the Chair of the Management Board.
11. Decisions taken by the Management Board will be made by consensus.
12. The Management Board Chair will submit a report to the Chair of the Business Mobility Group annually or as requested by the Chair of the Business Mobility Group.
13. The role of the Secretary of the Management Board will rotate annually amongst the participating economies.

ANNEX 2

**MODEL ECONOMY
MEMORANDUM OF UNDERSTANDING**

(REGIONAL MOVEMENT ALERT SYSTEM)

**MEMORANDUM OF UNDERSTANDING
BETWEEN**

[ECONOMY X]

AND

[ECONOMY Y]

**REGARDING LOST AND STOLEN PASSPORTS WITHIN THE REGIONAL
MOVEMENT ALERT (RMAL) SYSTEM**

THE GOVERNMENT OF [ECONOMY X] AND THE GOVERNMENT OF [ECONOMY Y] (hereinafter referred to as “the Participants”),

Recognizing that the urgent problems of border and transportation security arising from illegal immigration, international terrorism and other serious forms of international crime demonstrate the need for progress in co-operation among border protection, immigration, passport, and diplomatic agencies;

Desiring to make travel and entry to economies’ territories easier for legitimate tourists, students, and business travellers, while making it more difficult to travel to and enter the territories illegally;

Noting that one way to improve international border protection is the development of arrangements for the provision and use of relevant information among the agencies concerned;

Recognizing that, in order to act swiftly and appropriately, border control, immigration, passport and diplomatic agencies must be able to obtain reliable information from their counterparts abroad to verify the authenticity of passports and to identify passports that are no longer valid;

Further recognizing that, to the extent such information can be provided between and among economies, it can assist in preventing the travel and entry of inadmissible persons;

Further recognizing that this Memorandum of Understanding (MOU) aims to support and facilitate the provision and use of information on lost and stolen passports within the RMAL System (which operates under the auspices of APEC) and consistently with the RMAL System Multilateral Framework as well as the APEC Privacy Framework;

Further recognizing that nothing in the way this MOU is designed or implemented should affect the essential sovereign authority of each Participant to determine who is to enter its respective territory.

UNDERSTAND as follows:

SECTION I: PURPOSE OF MEMORANDUM

The purpose of this MOU is to establish the conditions under which the Participants intend to make available to each other information on lost and stolen passports within the RMAL System, to detect and prevent the misuse of those passports.

SECTION II: DEFINITIONS

A lost and/or stolen passport means any issued ECONOMY X or ECONOMY Y travel document that is lost, stolen, revoked, or otherwise invalid and any lost or stolen ECONOMY X or ECONOMY Y blank travel document.

SECTION III: RESPONSIBLE AGENCIES

The following entities are authorized to implement the provisions of this MOU: for ECONOMY X [insert], and for ECONOMY Y [insert].

SECTION IV: RMAL PROGRAM PROVISIONS

The following are mutually understood:

- A. The Participants intend to make available electronically the following four data elements: passport identification number, issuing authority, type of document, and the date of issuance as contained in their lost and stolen passport databases.
- B. The electronic availability should be on a real-time basis, to the extent practicable.
- C. Each Participant intends to maintain, on a 24/7 basis, the capacity to assist in establishing the validity or authenticity of a passport, to assist in determining subsequent action, and to field technical questions regarding the RMAL System.
- D. When a person presents a passport that matches against the data elements of the providing Participant, it should be evaluated for purposes of determining whether the passport holder will be permitted to travel or enter as described in Annex 1 of this MOU. In such cases, a participant should not take action based on concerns on the status of the passport until it has contacted the passport issuing authority and followed the procedures as described in Annex 1 of this MOU.
- E. The Participants may at their discretion provide additional information to each other, including personal/biographic information as appropriate, to assist in establishing the validity or authenticity of a passport and for the purpose of taking enforcement action related thereto.

SECTION V: TECHNICAL SPECIFICATIONS

A. Each Participant intends to make the data elements available to the other in a mutually acceptable electronic format and in a format that meets the RMAL System specifications. A technical working group (TWG) comprised of analysts from each Participant and other RMAL participating economies as appropriate should be established to develop the technical means to provide such data.

B. Each Participant intends to ensure that the data provided to the other Participant is as accurate, relevant, timely, and complete as is reasonably necessary to meet the specifications set out in Section IV.

SECTION VI: CONDITIONS OF USE

A. The information provided to the receiving Participant may only be used for one or more of the following official purposes:

1. To assist in determining whether an individual satisfies the legal requirements for a visa, entry, continued presence within the nation's territorial limits, or other citizenship, immigration or border management functions in relation to the use of a passport;
2. To prevent, detect, suppress, investigate, prosecute or punish criminal activity (including, but not limited to, passport offences, terrorism or trafficking in controlled substances, persons or illicit weapons), in relation to the use of the passport by an individual; or
3. To assist in the seizure of a lost or stolen passport.

B. The receiving Participant may disseminate the information provided under this MOU to agencies of that Participant only for the purposes specified in paragraph A of this Section, unless authorized in writing by the providing Participant. Within each receiving agency, each Participant intends to permit access only on a need-to-know basis.

C. Each Participant should notify the other of a dissemination made for a purpose specified in sub-paragraph A.2 of this Section.

D. In addition to a disclosure for a purpose specified in paragraph A of this Section, information received under this MOU may be disclosed where such disclosure is required by the law of the receiving participant.

E. The receiving Participant is to notify the providing Participant of any disclosure to be made in accordance with paragraph D of this Section. To the extent practicable, the receiving Participant should notify the providing Participant in advance of any such proposed disclosure to provide the opportunity, where appropriate, to the providing Participant to seek non-disclosure or other protection of the information to the extent permitted by the law of the receiving Participant

SECTION VII: SECURITY/SAFEGUARDS

A. The receiving Participant intends to use its best efforts to maintain any personal/biographical or other related information received in accordance with

Section IV in the same manner as it maintains like information concerning its own citizens. In the event that such information cannot be so maintained, the receiving Participant should inform the other of this fact and the reasons therefor.

B. Integrity of Information. Information provided and received under this MOU should be accurate, complete and kept up-to date to the extent necessary for the purposes of this MOU.

1. The Participants do not intend to modify any information received under this MOU without the authorization of the providing Participant.
2. When either Participant becomes aware that information it provided or received under this MOU is inaccurate, the Participant, subject to its domestic laws, is to advise the other Participant thereof and provide correct information. Upon receipt of such information, the receiving Participant should take steps to ensure that the inaccurate information is destroyed and/or to otherwise correct the information.

C. Security Administration. Each Participant should appoint a Systems Security Official. These individuals should have the authority to enforce the provisions of this MOU, subject to the Participant's domestic laws, pertaining to security and should act as agency contacts for that purpose.

D. Access Controls. Both Participants should have security safeguards in place (including electronic safeguards) controlling on a need-to-know basis access to information obtained under this MOU. Such safeguards should allow an audit trail that permits full identification of persons who have accessed the information.

E. Dissemination Controls. Both Participants should ensure that information that is obtained under this MOU is protected from unauthorized dissemination.

F. Prevention of Misuse. Each Participant is expected to take appropriate action under its administrative, civil, and criminal laws in the event of misuse, unauthorized alteration, deletion of, or access to or dissemination of information obtained under this MOU by its own employees, agents or any third party. In the event that such actions are taken, the Participant taking such action should notify the other Participant.

G. When a receiving Participant becomes aware of any attempts to inappropriately gain access to, use or disseminate information obtained under this MOU, whether by bribery, coercion, or other means, the receiving Participant should report in a timely manner, to the providing Participant's Systems Security Officer.

H. Records Storage. The Participants should at all times store information obtained under this MOU in a secure electronic storage system.

I. Retention of Information. Information obtained under Section IV.E should be retained only as long as necessary to carry out the purposes stated in Section VI.A. Each Participant should keep an audit record as to how long the information was held and when it was disposed of and should make such information available to the other Participant if requested.

J. In the event that the Participants cease to participate with each other in the RMAL system for whatever reason and terminate this MOU, the Participants should dispose of all information obtained from each other as a result of the operation of the RMAL System in accordance with their domestic laws, unless otherwise agreed in writing.

K. Personnel Training for Permitted Uses. Each Participant should ensure that all of its personnel with access to data and other information obtained under this MOU are trained in the safeguards required to protect such information.

L. If in the view of a Participant sufficient safeguards are not being maintained by the other with regard to the information provided under this MOU, it may withhold provision of further information pending a resolution of the issue under Section XI.

M. As necessary, each Participant may request assurance from the other that sufficient safeguards are being maintained by the other with regard to the information obtained under this MOU.

SECTION VIII: PRIVACY ISSUES AND COMPLAINTS

A. Each Participant should have a procedure whereby members of the public may raise privacy questions and concerns regarding the information that is provided pursuant to this MOU, through a designated point of contact for public enquiries as specified in Annex 1 of this MOU. Each Participant is to refer persons raising privacy questions or concerns about information provided under this MOU to the designated point of contact of the Participant that provided the information, to the extent that such referral is appropriate and permitted by law.

B. Privacy questions and concerns should be considered and responded to in a timely manner by the Participant to which they are addressed, and in accordance with applicable laws of that Participant.

SECTION IX: RMAL SYSTEM MANAGEMENT BOARD

The Participants each intend to maintain a representative on the RMAL System Management Board, which is to provide strategic and operational governance of the RMAL System consistent with the RMAL System Multilateral Framework document and having regard to domestic legal obligations of each RMAL System participant. Each Participant intends to act in accordance with the guidance of the RMAL System Management Board and the protocols and standards it sets, to the extent practicable and permitted by applicable law.

SECTION X: CONTACT PERSONS

Each Participant should appoint one or more RMAL System Administrators (of appropriate seniority within the authorized implementing entities), in addition to a Systems Security Officer, and provide the other Participant with the details of their Administrator(s) and Security Officer (including their contact information) by way of exchange of letters.

SECTION XI: CONSULTATIONS

The participants, through their RMAL System Administrators, should consult as necessary to promptly address and endeavour to resolve any issues arising under this MOU or the operation of the RMAL System.

SECTION XII: AMENDMENT

A. Either Participant may request amendment of this MOU at any time by writing to an RMAL System Administrator of the other Participant.

B. This MOU may only be amended by the written consent of both Participants, except that Annex 1 of this MOU may be amended by the written consent of RMAL System Administrators from both Participants.

C. In any case where an amendment to Annex 1 is proposed, the RMAL System Administrators should ensure that;

1. The proposed amendment is consistent with the principles of the RMAL System Multilateral Framework and the RMAL System as well as the APEC Privacy Framework;
2. Appropriate processes have been followed and authorities obtained within their own economies for the amendment;
3. The RMAL System Management Board has the opportunity to comment on the proposed amendment before it is finalised and is provided with a copy of the final amendment.

SECTION XIII: STATUS OF MOU

A. This MOU embodies the understanding of the Participants. It is not governed by international law and does not create legal obligations.

B. The provisions of this MOU should not prevent either Participant from cooperating or granting assistance in accordance with the provisions of other applicable international treaties and agreements, arrangements, national laws and related practices.

C. Nothing in this MOU is intended to supersede the obligations of the Participants to report lost and stolen passports to the Interpol database of lost and stolen travel documents by the end of 2006, as detailed in the Joint Ministerial Statement of 16 November 2005 and endorsed by the APEC leaders in the Busan Declaration of 19 November 2005.

D. This MOU is not intended to create or confer any right or benefit on any person or party, private or public.

SECTION XIV: COMMENCEMENT AND TERMINATION

This MOU should come into effect upon signature and may be terminated by either Participant upon written notice to the other Participant.

Signed at _____, in the English language, this ____ day
of _____, 2006.

*FOR THE GOVERNMENT OF
ECONOMY X*

*FOR THE GOVERNMENT OF
OF ECONOMY Y*

**MEMORANDUM OF UNDERSTANDING
BETWEEN**

[ECONOMY X]

AND

[ECONOMY Y]

**REGARDING LOST AND STOLEN PASSPORTS WITHIN THE REGIONAL
MOVEMENT ALERT (RMAL) SYSTEM**

Annex 1

Permissible Actions

I. Introduction

1. These Permissible Actions cover the following passenger movements:
 - a. [Economy X] travel document holders travelling to or seeking to enter [Economy Y] [from the last point of embarkation]; and
 - b. [Economy Y] passport holders travelling to or seeking to enter [Economy X] [from the last point of embarkation].

II. Notification and Verification Arrangements

1. When a person presents a passport which is listed by the issuing authority as lost, stolen or otherwise invalid, the immigration authority (agency name) intends to notify the 24/7 Office of the issuing authority for that passport (agency name).
2. This notification should be accompanied by the following information:
 - a. travel document number,
 - b. name of bearer,
 - c. port of embarkation, and
 - d. airline, flight number and departure time.
3. For making decisions about authorization of inward travel or entry in cases where an initial match of the data elements occurs, an immigration authority should not take action based on concerns on the status of the passport until it has contacted the passport issuing authority. This is to ensure that prior to a decision being made, Participants can verify that the "hit" did not occur as a result of data errors or data inaccuracies, and that legitimate travellers are not unnecessarily hampered.
4. 24/7 passport authority office managers retain discretion whether to provide further information, including personal/biographical information as appropriate, to assist in verifying the validity and authenticity of the passport.
5. 24/7 immigration authority office managers retain discretion whether to permit entry or advise airlines to permit boarding.

6. The immigration authority should report to the passport authority any adverse action taken against the bearer of a passport.

III. Procedures

1. Each immigration and passport authority should establish operational procedures for managing different situations and, as a matter of courtesy and goodwill, advise the other Participant of its procedures. These operational procedures should include mechanisms for:
 - a. ensuring that legitimate travellers are not unnecessarily delayed;
 - b. preventing the travel or entry of those engaged in terrorism, illegal immigration and other serious crimes; and
 - c. seizing passports which are being used illegally with the ultimate aim of returning them to the issuing participant.

IV. Administration/Reviews

1. To ensure consistency of treatment of each Participant's citizens and to improve operational procedures, the program administrators of the agencies involved in the implementation of the MOU should periodically consult regarding the implementation and terms of this Annex and any systems, policy and operational matters associated with it.
2. These consultations should take place at 3 month intervals for the first year of its implementation. After the first year, consultations should take place on an as needed basis, by mutual consent.

V. Points of Contact

1. 24/7 points of contact are to be the following:
 - a. for [Economy X]
 - b. for [Economy Y]
2. Points of contact for public inquiries (including privacy questions or concerns) are to be the following:
 - a. for [Economy X]
 - b. for [Economy Y]