Regional Advanced Passenger Information Opportunities for PICTs

RESEARCH

Prepared by: Coordinated Border Solutions (Haddon Wright and Peter Speldewinde) for PIDC

www.coordinated-border.solutions

Date: 14th October 2021

Contents

Acronyms and Expressions Used

ACP – African, Caribbean and Pacific Group of States

API – Advance Passenger Information

APIS - Advance Passenger Information System

APP – Advance Passenger Processing, closely related to iAPI

ARINC - Aeronautical Radio, Incorporated, now a Collins Aerospace subsidiary/brand

ASYPX – the UNCTAD Passenger Processing Module

Batch API – this is a mode of one-way API data transmission from carriers to recipient Government agency/ies in a single batch of data, typically as embarkation or boarding closes and prior to departure from the port of embarkation

BMS – Border Management System - the IT system(s) which support Immigration and Border Control

CARICOM – the Caribbean Community

CBM – Coordinated Border Management – synonymous with "Integrated Border Management"

Chicago Convention – the 1944 *Convention on International Civil Aviation*

Craft – means any means of aircraft or vessel capable of crossing an international air or maritime border.

DCS – Departure Control Systems (employed by air carriers)

ETA – Electronic Travel Authority

EU – European Union

e-Visa – electronic visa

FAL 65 – the 1965 Convention on Facilitation of International Maritime Traffic

iAPI – Interactive Advance Passenger Information. Closely related to APP, this is a mode of two-way API data exchange between a carrier and recipient Government agency/ies, whereby individual API data is transmitted by carriers as each traveller checks in, and a response is sent within a few seconds from the recipient Government agency with an assessment result, typically "board" or "do not board".

IATA – the International Air Transport Association

IBMS – Integrated Border Management System/s

ICAO – International Civil Aviation Organisation

IMPACS – the CARICOM Implementation Agency for Crime and Security

INTERPOL – the International Criminal Police Organisation

IOM – International Organization for Migration

JRCC – the Joint Regional Communications Centre, a sub-agency of CARICOM's IMPACS, responsible for the management of the regional APIS

MIDAS – IOM's Migration Data Management, Intelligence and Risk Analysis system

MRTD – Machine-readable Travel Document

PDSW – Passenger Data Single Window, referred to in standard 9.1, Annex 9, Chicago Convention

PICP - Pacific Islands Chiefs of Police

PICT – Pacific Island Country and Territory

PIDC – Pacific Immigration Development Community

PIF – Pacific Island Forum

PNR – Passenger Name Record

PTCCC - Pacific Transnational Crime Coordination Centre, part of the Pacific Transnational Crime Network

RTAC – a term coined only in this report, referring to a proposed Regional Traveller Assessment Centre. Such a centre could be named in any other way as preferred by participants.

SITA - Société Internationale de Télécommunications Aéronautiques

SLTD – the Interpol Stolen and Lost Travel Document database

TCU – Trans-national Crime Unit, national units of the Pacific Transnational Crime Network

UNSC – United Nations Security Council

UNSCR - UNSC Resolution

Visa – the legal authority issued by a country or territory to permit the travel to, entry, and/or stay of a non-citizen. In this report the term includes the concept of "permit" which also exists in the legislation of several PIDC members.

WCO – World Customs Organization

Executive Summary

This paper has been prepared by Coordinated Border Solutions (CBS) at the request of the Pacific Immigration Development Community (PIDC), on possible opportunities for PIDC members to access Advanced Passenger Information (API). It draws upon extensive research into international and regional best practice with similar arrangements, consultation with a range of government and non-government stakeholders in the Pacific and elsewhere, and the broad experience of the CBS authors.

Implementation of API is a high priority for the international community given its ability to substantially enhance the ability of border agencies to understand the identity and intent of individual travellers, and thus the level of risk posed by them. This in turn unlocks significant enhancements to national, regional, and global border and transportation security, countering irregular migration, transnational-crime, terrorism, and offers the potential to assist with health screening.

Mandated via several UN Security Council Resolutions since 2014, and Annex 9 of the Chicago Convention, implementation is not only an obligation, it serves the interests of the region. Implementation has, however, been slow, mainly due to genuine gaps in systems, human and financial constraints, perceived complexity, and in many cases, lack of enabling legislation.

API implementation appears at first to be deceptively simple, consisting of an electronic set of standardized data relating to travellers, which can take the form of a spreadsheet. The complexity lies in making best use of the data, which requires a 24/7 human assessment capability, preferably a Border Management System (BMS), as well as profiling and rules-based assessment tools connected to key international databases such as those of the International Criminal Police Organisation (Interpol). The challenges faced by Pacific Island Countries and Territories (PICTs) to individually configure, deploy and utilise these tools, and effectively staff a round-the-clock assessment centre remain difficult to surmount.

The Boe Declaration of 2018, and its supporting Action Plan elaborate regional mechanisms in respect of the increasingly complex security and transnational crime environment, and the creation of an enabling environment for implementation of regional responses including an appropriate coordination mechanism. The language in both documents provides a clear indication that establishment and strengthening of regional coordination mechanisms which support the national security and sovereignty of members in response to these threats, is fully supported by Pacific Island Forum (PIF) leaders.

Consistent with these principles, this paper outlines:

    a) possible models for the implementation of API by PIDC Members;
    b) implementation pathways with or without a national BMS;
    c) the means of integration with assessment tools and international law enforcement databases;
    d) possible opportunities for cost and resource sharing amongst the PIDC membership to enable broad implementation; and
    e) suggested enabling amendments to the Immigration legislation of PICTs to provide the legal authority for the introduction of API.

1. Introduction and Background

The management of people movements across borders is an important policy priority for most countries due to an emerging range of concerns including; pandemics, the global spread of terrorism and trans-national crime, the (pre-COVID) growth in international tourism, ageing populations, and the occurrence of skills gaps in domestic labour forces. As a consequence, Governments around the world claim the sovereign right to carefully determine which individuals are permitted to cross their national borders. Effectively, they seek to prevent those who are assessed as posing a risk from entering their country or, in certain circumstances, departing. These risks can be direct threats - such as people with contagious diseases, criminals or people of security concern - or risks posed by those who intend to behave in a manner contrary to the law or policy of the country concerned - such as people who are the subject of an arrest warrant, preach sedition and sow social discontent, intend to work without authority, or to overstay the time allowed for their visit.

It is because of these risks, and the fact that there exist several opportunities to confirm the identity and intent of travellers, that many countries have moved towards a 'layered' checking approach to travellers seeking to cross their borders. Contemporary thinking on effective border control has moved away from the traditional definition of a border as being the limit of two countries' sovereignties—or the limit beyond which the sovereignty of one country no longer applies. As the World Bank highlights, borders no longer need to be at a country's geographic periphery, are not holistic, and can even be located outside a country.[1]

The power to approve or refuse the entry, stay or departure of a person can be exercised in four different contexts:

- offshore - where a person is required to apply for and be granted a visa prior to travel. The capacity of PIDC members to utilise this feature is limited due to the low level of off-shore representation and relatively poor BMS and IT infrastructure;
- offshore – where a person is screened as part of the check-in process before they board a flight or a ship to travel to their destination country;
- onshore – when a person arrives at an airport, seaport or border post; and
- onshore – when a person has already entered the country and is applying for further stay, is subject to immigration law enforcement, or is the subject of a Court or other prohibition order.

In terms of the entry of people, logic suggests that the ideal time to exercise this power is offshore before the passenger departs their country of origin - either by not granting them a visa or by screening them and refusing permission to board. This mitigates most immigration and law enforcement risks and costs in the destination country. Early intervention also avoids cost and risk to other stakeholders, notably carriers, who are generally responsible for removal costs for those refused entry at their destination, and also the travellers themselves.

---

[1] World Bank – Border Management Modernisation, 2011, page 37. Available at http://documents.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf

By definition, border controls and immigration arrangements have never been unilateral, solely internal matters, as they always involve at least one other country (for example the border control arrangements between the US and Canada, those between Australia and New Zealand and to a lesser extent APEC) and, most often, a carrier. This requires an established set of standards and some level of coordination and communication of arrangements between the parties.

What has emerged is the concept of a 'border continuum', in which the actions of people preparing to travel, actually travelling, arriving, remaining within the destination country, and departing, are integral parts of the border management process. However, early intervention is dependent on the level of visibility a border management agency has on the travel process of passengers and the time available to them to make informed clearance decisions.

In the 21st Century, there is a variety of Border Control Agencies in place at most official ports of entry/departure, including in the Pacific. These include Immigration, Customs, Police, Quarantine, Health and Safety, Agriculture and so on. The level of co-operation between these Border Control Agencies varies from place to place. Different agencies may operate their own automated systems for passenger processing without any sharing of information. The strict division of responsibilities between the agencies means that passenger processing is often unnecessarily prolonged and there is often duplication in the information travellers are required to provide.

API is a highly effective tool used by an increasing number of countries to enhance controls over passengers, while maintaining facilitation for low-risk passengers, to the benefit of Immigration, Customs and other Border Control Agencies, Carriers, Airport Authorities (and other passenger facility operators) and passengers themselves. API involves the capture of a traveller's biographic data and other travel details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. There, they can be screened against their immigration and enforcement database(s) to identify high risk passengers requiring, for example, more intensive questioning upon arrival. It therefore has the potential to considerably reduce inconvenience and delay experienced by some passengers as a result of necessary border processing and also provides a system that carriers can use to comply with relevant legislation of the countries into which they fly. A more fulsome discussion of API is at section 2.1 of this report.

1.2   Assumptions

For the purposes of this paper the authors have assumed:

1. Moderate post-COVID increases in the number of traveller movements over time, albeit with some volatility.

2. Land border management is not a significant issue for most PICTs.

3. The most significant issues that need to be addressed relate to the two highest volume channels: the swift and effective processing and clearance of travellers arriving by air and via cruise ships.

4. All PIDC members are committed to adopting API and related identity management and information sharing arrangements because they are mandated under United Nations

Security Council Resolutions (UNSCRs) 2178, 2309 and 2396, and Chapter 9 "Passenger Data Exchange Systems", in Annex 9 of the Chicago Convention[2], to which they are all signatories.

5. The features of international travel in the Pacific, including the needs of PICTs and the expectations of travellers, while increasingly complex, are not likely to be subject to major changes to the operating or policy environments.

1.3   Methodology

In preparing this report CBS:

- researched and analysed a wide range of available material on the development and best practice use of API, Passenger Name Record (PNR) and interactive Advance Passenger Information (iAPI) arrangements as well as bringing to bear direct experience in border management in Europe, the Middle-East, Asia, North America, and the Pacific;

- conducted an environmental scan to identify examples of the operation of arrangements involving the use of API/PNR/iAPI by individual states and groups of countries including conducting a series of virtual meetings with a range of organisations, for example the Caribbean Community (CARICOM) and Société Internationale de Télécommunications Aéronautiques (SITA) (see Chapter 4 below for a more fulsome discussion);

- undertook an analysis of PIDC members' Immigration legislation to determine whether they currently have the legislative authority to collect and share information, and also assessed what may be necessary in terms of legislative change to lawfully support the introduction of API and information sharing more broadly (see **Annex 1**);

- developed a model set of Immigration Act amendments to introduce the necessary Heads of Power to create the legislative authority to share information in support of the possible introduction of API, as well as a model set of Regulations which prescribe the format and controls applying to the sharing of information and, specifically, the operation of API (see **Annex 2**); and

- drew upon feedback and opinions about the operation of the current immigration arrangements received from both government and non-government stakeholders during an extensive series of face-to-face consultations undertaken in several Pacific countries including Cook Islands, Federated States of Micronesia (FSM), Tonga, Tuvalu, Samoa, Solomon Islands (Solomon's) and the Republic of the Marshall Islands (RMI). A synthesis of the feedback, as it relates to the collection, storage and sharing of information, is at **Annex 3**.

---

[2] Available at https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

2. Introduction to Advance Passenger Information (API)

2.1   What is API?

Advance Passenger Information, otherwise known as API, evolved in response to the significant growth in air travel in recent decades, the reality of increasingly stretched border control agencies, along with new security threats such as global terrorism, identity fraud, and trans-national organised crime.

API involves the capture of a passenger's biographic data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. It may also be required for departing aircraft by the country of embarkation, although the imperative for this is lessened as much of this data is already captured by departure immigration controls.

API is generally employed by receiving Governments as a decision-making tool that Border Control Agencies can utilise before a passenger is permitted to board an aircraft and before they arrive. API can also be utilised for maritime movements, from large cruise ships to small craft such as yachts.

Air carriers, and an increasing number of maritime carriers support API because it also provides them with a system which they can use to ensure compliance with relevant legislation of the countries they fly or sail into, reducing fines, penalties, and refused entry situations.[3]

Why is API important?

API, along with measures such as Electronic Visas (e-Visas) or Electronic Travel Authority (ETA) arrangements hold out the prospect of being able to "push the border out", with the vast majority of travellers identified and assessed as to risk prior to travel.

Traditionally a border has been defined as the limit of two countries' sovereignties—or the limit beyond which the sovereignty of one country no longer applies. However, the concept of a border has changed in recent years. As the World Bank highlights, borders no longer need to be at a country's geographic periphery, are not holistic, and can even be located outside a country.[4]

Airport and seaport arrival processing arrangements which are commonplace in the Pacific form part of what is described in contemporary literature, as a 'border continuum', in which the actions of people preparing to travel, actually travelling, arriving, remaining within the destination country, and departing, are integral parts of the border management process. Arrival processing should be enabled by comprehensive information on passengers, received in advance of their

---

[3] Text significantly adapted from WCO – Guidelines on API, 2010, paragraph 3.8, at
https://www.icao.int/Security/FAL/Documents/2010%20API%20Guidelines%20Final%20Version.ICAO.2011%20full%20x2.pdf
[4] World Bank – Border Management Modernisation, 2011, page 37. Available at
http://documents.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf

arrival, supported by a well-managed targeting and alerts system, and contribute to the interests of a range of agencies at the border and beyond.

By definition, border controls and immigration arrangements have never been unilateral, solely internal matters, as they always involve at least one other country (for example the border control arrangements between the US and Canada, those between Australia and New Zealand and to a lesser extent APEC) and, most often, a carrier. This requires an established set of standards and some level of coordination and communication of arrangements between the parties. In a perfect world a system such as that presented at Figure 1 below, would provide opportunities for border agencies to intervene in respect of particular passengers at the time and place which offers the best chance to avoid any potential harm to the country of destination and at the lowest possible cost.

After arrival - Within the country (visa extensions, compliance etc)

Prior to final clearance at a port (Customs baggage checks, Quarantine checks etc)

Arrival - Presentation at the border (the Primary Line)

Travel commencement - Check-in overseas with an airline or shipping company, immigration departure control

Pre-travel - Visa application & ticketing overseas
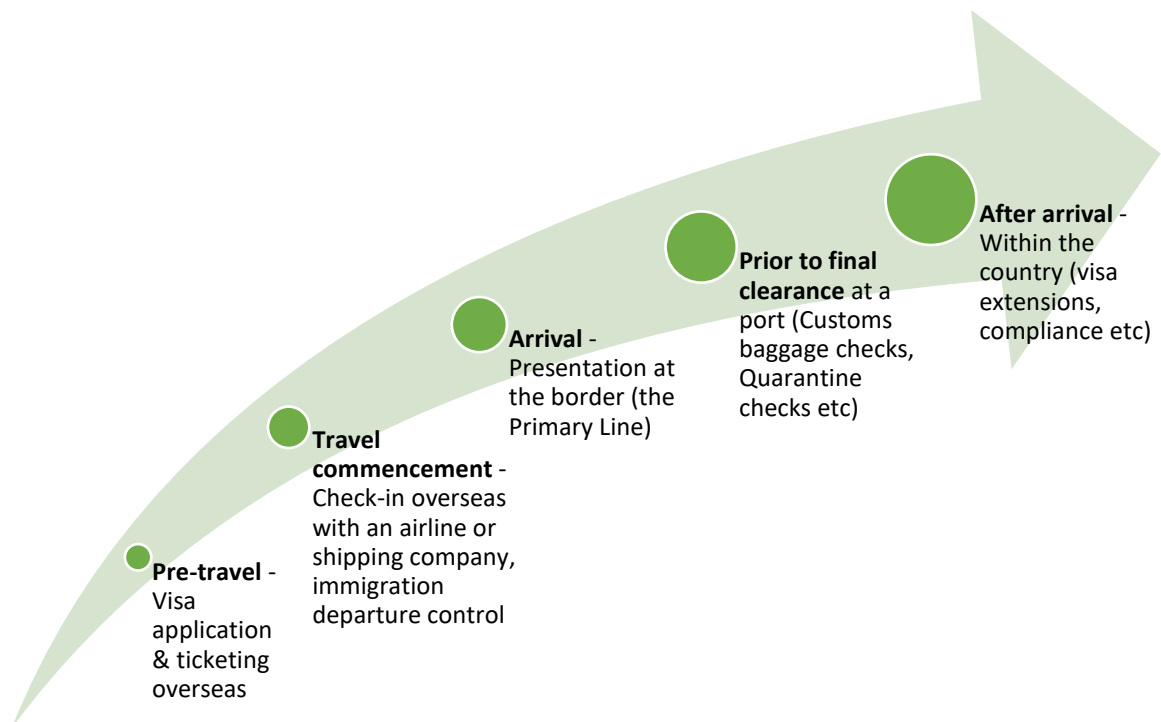
Figure 1: Layered approach to intervention along the border continuum

Regardless of the nationality or status of travellers, the core objectives of Immigration and any delegated border agencies undertaking arrival and departures functions must be to:

- **establish the traveller's identity; and**
- **determine the traveller's intent.**

Figure 2: Traveller identification and risk assessment

Establishing the identity of travellers enables other objectives to be met, including entitlement verification and risk assessments (as represented at Figure 2) of individuals by all involved agencies, and contributes to the assessment of traveller intent (why they are seeking to cross a border).

The deployment of API assists in meeting these objectives. It does not operate as an end to itself but usually forms part of a multi-agency approach to the pre-assessment of travellers.

Once passengers are cleared for boarding, details are then sent to the Border Control Agencies for screening against their immigration, customs, and any other enforcement database(s). This can identify high risk passengers requiring for example more intensive questioning upon arrival. If time permits, passengers of concern can even potentially be prevented from boarding or be offloaded from a flight to prevent their travel.

API has the potential to considerably reduce the inconvenience and delay experienced by most passengers because necessary border processing and risk assessment can often be completed before they arrive. Travellers pre-assessed as low-risk can be accorded a "light touch" on arrival, with the limited resources available to agencies at ports of arrival targeted at pre-identified higher-risk travellers aboard. [5]

How is API data generated?

The International Civil Aviation Organisation (ICAO), / World Customs Organisation (WCO) / International Air Transport Association (IATA) provide the following useful summary of how passenger data, including API data, is generated by airlines:

"The flow of passenger-related information from Carriers to border control authorities can be divided into three main streams:

1. Passenger Name Record

A reservation can be made from approximately 360 days before departure till the moment that the check-in process is stopped, which is approximately 2-3 hours before departure (depending on the airport and route).

2. Passenger Manifest Information from the Departure Control System

Approximately 48 to 36 hours before departure all PNRs are transferred from the Airline Reservation System to the Departure Control System (DCS). In the DCS the operational handling of the flight will take place, at check-in (e.g., intake of baggage and issuing of Boarding passes). It

---

[5] Figure from the ICAO TRIP Guide - https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx

is common use that a passenger manifest is forwarded to the airport of destination for operational purposes (passenger and baggage handling)

3. Advance Passenger Information from the Departure Control System

As API data is not generally required for Airline processes, it will normally be collected and stored only in case of a legal requirement. There are three methods employed to collect the required information depending on the timeframe for the provision of this data:

a) at the moment of reservation, by the passenger and/or his travel agent (manually entered into the reservation record);
b) at the moment of check-in, by the passenger at Internet check-in (manually entered into the API section of the DCS), by the passenger at kiosk check-in (automated from the machine-readable zone), or by the Airline agent at desk check-in (automated from the machine-readable zone);
c) at the moment of boarding, by the Airline agent (automated from the machine-readable zone).

Whilst API data registration by the passenger at the moment of reservation is operationally the most convenient for carriers; manually entered information has the risk that incorrect information is supplied (e.g., a zero instead of the letter O). The best option from a data quality perspective is the collection of the machine-readable information, via an automated process."[6] This is generally at check-in.

Types of API

There are two main types of API

Batch API – this is a mode of one-way API data transmission from carriers to recipient Government agency/ies in a single batch or list of data, typically as embarkation or boarding closes and prior to departure from the port of embarkation. This is the simplest form of API to implement, and is the most commonly deployed form.

Interactive Advance Passenger Information or iAPI - closely related to Advance Passenger Processing (APP), this is a mode of two-way data exchange between a carrier and recipient Government agency/ies, whereby individual API data is transmitted by carriers as each traveller checks in, and a response is sent within a few seconds from the recipient Government agency with an assessment result, typically "board" or "do not board".

Whilst a final consolidated API batch or list may also be sent prior to take-off, it can be seen that the value inherent in this approach is carriers obtain a "live" response from the receiving Government, increasing the security and compliance outcomes for both the Government and the carrier.

---

[6] ICAO WCO IATA Management Summary on Passenger-related Information Umbrella Document) – located at https://www.icao.int/Security/FAL/Documents/Umbrella_Document.2013Dec03.pdf

How complex is API?

The key principles of API are that the data is:

- electronic, not hardcopy; and
- in a standardised format.

Because of its one-way nature, batch API is simpler to implement, whilst still delivering most of the border risk management and security outcomes sought by Governments.

At its most basic level, batch API can take the form of an emailed spreadsheet, sent from a carrier or captain or master of a craft to a designated email address of the receiving Government agency. This method is often still used by major destination countries for small or private craft.

The information can then be manually uploaded into any system or analysis tool, such as an enabled Immigration BMS to verify traveller status (presence of a visa, citizenship, national passport validity, alert list matches), as well as any API assessment tool which may exist, and other systems such as those of Customs, Police and Security Service databases for recording and checking against their warning lists or profiles.

It is important that the data is electronic, not hardcopy. Hardcopy manifests, which are commonplace in countries without API, do not lend themselves to easy analysis. This can only be done using hand keyed data entry to check against systems, or manual visual checks, or worse, not at all due to the tedious and labour-intensive nature of this approach when airports are busy.

Hardcopy manifests are also often in the preferred individual format of the airline or shipping agent, and are thus not standardised. Even basic biodata such as full family and given names, date of birth and passport number and nationality is often missing from hardcopy manifests, making data matching very difficult.

A standardised data format has been established by ICAO, WCO and IATA, known as UN/EDIFACT PAXLST, which ensures that API data fields requested are internationally accepted, and key variable data such as country, port and airline details are easily referred to by internationally recognised standard codes.[7]

Whilst some API data may be transmitted by email as detailed above, more often it is transmitted via either a direct carrier-Government link, such as a VPN link or similar, or more commonly for air carriers, via one or more of the major airline communication and passenger management system providers such as SITA or Aeronautical Radio, Incorporated (ARINC). The latter are commonly utilised as they have extensive experience in the collection and transmission of both batch and interactive API data from airline DCS, and are generally already utilised by carriers for their broader reservation, ticketing and/or passenger management requirements.

The use of networks such as those of SITA and ARINC for reception of API data does (generally) require some integration with Border Management Systems, which these companies can usually assist with, however this assistance does come at a cost which may prove problematic for smaller PICTS or agencies.

---

[7] See the WCO API Guidelines at http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx?p=1

iAPI is by definition more complex to implement, as it requires significant systems integration between the Government BMS systems, and airline DCS. Reliable secure two-way communications are also required, which are accessible to and trusted by both Governments and carriers alike. iAPI responses from Governments to carriers follow a standardised ICAO, WCO and IATA format known as CUSRES.

For this reason, iAPI implementations generally rely heavily on the SITA and/or ARINC networks, and being more complex, attract a higher cost per traveller from the network providers.

iAPI also requires greater sophistication on the part of Government systems such as BMS, as they often involve automated data import and checking, and may even involve computer-aided decision-making.

Recommendation 1: Batch API is recommended for any initial API implementation in the Pacific.

Recommendation 2: Consideration should only be given to the implementation of iAPI once the human, systems, and legislative capability within agencies and Governments has adapted and expanded to effectively accommodate Batch API.

How is API different to PNR?

Advance Passenger Information refers to a passenger's identity and includes full name, date of birth, gender, citizenship and travel document data. API is typically obtained from travel documents and available from the machine-readable area of a traveller's passport as specified in ICAO Document 9303. As mentioned above, API data is not generally required separately for Airline processes, and it will normally be collected, transmitted and stored separately only in case of a legal requirement.

Passenger Name Record information is the generic name given to records created by the airlines for each flight booked by a passenger. PNR records contain information provided by the passenger and information used by airlines for their operational purposes. PNR information may include elements of information that will also be reported under API. PNR provides a mechanism for all the different parties within the aviation industry (including travel agents, air carriers and handling agents at airports) to recognize each passenger in a common format, and have access to all information relevant to his/her journey, departure and return flights, connecting flights (if any) and special services required on board the flight.

The amount and the nature of the information in a PNR record can vary from airline to airline and from passenger to passenger, often depending on how the reservation was made. A PNR may contain as little information as a name, or may contain full address, contact details, credit card information and all data pertaining to the booking. [8]

---

[8] As above, and also from ICAO website summary at
https://www.icao.int/security/fal/sitepages/api%20guidelines%20and%20pnr%20reporting%20standards.aspx

As the data may be more personal in nature, PNR data is subject to more stringent regulation by, among others, the European Union (EU), which restricts the purposes to which PNR data may be put, to whom it may be transmitted, and how long it may be retained. This applies to PNR data which is in any way within EU jurisdiction, which can include PNR data stored by airlines on databases located there (such as reservation systems), even if it does not relate to flights to, from, or within the EU. [9]

It is because of this latter point, and the requirement by the EU that PNR data access is subject to individual bilateral agreements with countries that PNR is not recommended for inclusion in the initial implementation of API in the Pacific.

The WCO/ICAO/IATA standard form of transmission for API data is the UN/EDIFACT PAXLST format, and for PNR, the PNRGOV format. [10]

Recommendation 3: The adoption of PNR should only be considered once the human, systems and legislative capability within agencies has adapted and expanded following API implementation.

2.2. The Regional and International Legal Framework

Mandatory API

International law has grown to support increased carrier obligations and information sharing between Governments and the collection and transmission of traveller information from carriers to Governments.

This has occurred via the *Convention on International Civil Aviation* (also known as the *Chicago Convention*), and additionally via several UNSCRs including in particular:

- UNSCR 2178 (2014), which was adopted in response to the threat stemming from the travel of foreign terrorist fighters. Measures to be taken by Member States pursuant to resolution 2178 include:
  - Requiring that airlines operating in their territories provide API to the appropriate national authorities.
- UNSCR 2309 (2016):
  - Calls upon states to require that airlines operating in their territories provide API to the appropriate national authorities
  - Calls upon States to ensure the security of civil aviation by, implementing ICAO Annex 9 "…*standards and recommended practices relevant to the detection and prevention of terrorist threats involving civil aviation.*"

---

[9] See further detail of EU regulations at https://www.consilium.europa.eu/en/policies/fight-against-terrorism/passenger-name-record/
[10] See the ICAO Guidelines at
https://www.icao.int/security/fal/sitepages/api%20guidelines%20and%20pnr%20reporting%20standards.aspx

- UNSCR 2368 (2017), which reaffirms its call upon Member States in resolution 2178 (2014) to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities, and calls upon Member States to develop the capability to process PNR data and to ensure PNR data is used by the relevant national competent authorities.

These resolutions enable and mandate the sharing of information and expansion of measures such as API and PNR data to assist carriers in preventing the travel of persons of security concern.

Annex 9 of the Chicago Convention

ICAO presides over the formulation and adoption of Standards and Recommended Practices (SARPs) for international civil aviation. These are incorporated into the 19 technical annexes to the *Chicago Convention*.

Annex 9 to the *Chicago Convention* embodies the SARPs and guidance material pertaining specifically to the facilitation of landside formalities for clearance of aircraft and passengers, goods and mail, with respect to the requirements of customs, immigration, public health and agriculture authorities.

As such, it provides a frame of reference for planners and managers of international airport operations, describing the obligations of industry as well as the minimum facilities to be provided by governments. In addition, Annex 9 specifies methods and procedures for carrying out clearance operations in such a manner as to achieve compliance with States' laws while enabling maximum productivity for the air transport operators, airports and government inspection agencies involved.

Chapter 9 of the Annex deals specifically with ***Passenger Data Exchange Systems***, including API and PNR, as well as the data standards which should apply, thus making implementation easier for Governments and carriers.[11]

Adoption of API, and ultimately PNR data exchange with carriers forms part of ICAO's Traveller Identification Strategy. [12]

---

[11] See the text of Annex 9 at https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf , and API/PNR standards at https://www.icao.int/Security/FAL/ANNEX9/Pages/Publications.aspx
[12] See the TRIP Strategy documentation at https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx

Figure 3: ICAO Traveller Identification Strategy - partners and stakeholders

According to ICAO, *"…at the centre of the ICAO TRIP Strategy is the key proposition for States, ICAO and all stakeholders to address, individually and collectively: that a holistic, coherent, coordinated approach to the interdependent elements of traveller identification management is essential, encompassing the following elements:*

- *Evidence of identity – credible evidence of identity, involving the tracing, linkage and verification of identity against breeder documents to ensure the authenticity of identity;*
- *Machine-readable travel documents (MRTDs) – the design and manufacture of standardized MRTDs that comply with ICAO specifications;*
- *Document issuance and control – processes and protocols for document issuance by appropriate authorities to authorized holders, and controls to prevent theft, tampering and loss;*
- *Inspection systems and tools – inspection systems and tools for the efficient and secure reading, recording and verification of MRTDs, and*
- *Interoperable applications – globally interoperable applications and protocols that provide for timely, secure and reliable linkage of MRTDs and their holders to available and relevant data in the course of inspection operations."*[13]

By virtue of UNSCRs 2178, 2309 and 2396, and the standards at Chapter 9 "Passenger Data Exchange Systems", in Annex 9 of the Chicago Convention[14], **adoption of API and related identity information sharing is technically mandatory** for all Chicago Convention signatories, which includes PICTs[15].

---

[13] Text and diagram from the ICAO TRIP Strategy, https://www.icao.int/Security/FAL/TRIP/Pages/default.aspx
[14] Available at https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf
[15] See ICAO's API Implementation pathway at
https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20API%20Brochure_2018_web.pdf

> **Recommendation 4:** PIDC members should note that, while ETA or pre-clearance measures, PNR and Interpol SLTD[1] interoperability are not mandatory, they are recommended by ICAO and/or the United Nations Security Council (UNSC).

Single Window for Passenger Information

In 2018, Dutch authorities proposed an amendment to Annex 9, Chapter 9, to create a (mandatory) standard 9.1 to the effect that "*States requiring the exchange of Advance Passenger Information (API),/ interactive API (iAPI) and/or Passenger Name Record (PNR) data from aircraft operators shall create a **Passenger Data Single Window** facility for each data category or both data categories combined that allows parties involved to lodge standardized information with a common data transmission entry point for each category to fulfil all related passenger and crew data requirements for that jurisdiction.*".[16]

The Dutch proposal included lessons learned from that jurisdiction, in which it was clear that moving to a Single Window arrangement is easier when this is done deliberately at the beginning.

The proposal also contained a recommendation that any Passenger Data Single Window facility should cater for both data categories combined.

This recommendation was adopted by ICAO via amendment 27 to Annex 9 – Facilitation, which was anticipated to become effective on 21 October 2019 and to become applicable on 21 February 2020.

The Passenger Data Single Window amendments to Annex 9 are important and relevant as they provide a legal and technical precedent of considerable value to PICTs as will be seen below.

The Regional Mandate for Security Cooperation

In the Boe Declaration of 2018, the PIF stated that in addressing an increasingly complex regional security and transnational crime environment, the leaders "*commit to strengthening the existing regional security architecture inclusive of regional law enforcement secretariats and regional organisations to:*

> *a. account for the expanded concept of security;*
> *b. identify and address emerging security challenges;*
> *c. improve coordination among existing security mechanisms;*
> *d. facilitate open dialogue and strengthened information sharing;*
> *e. further develop early warning mechanisms;*
> *f. support implementation;*
> *g. promote regional security analysis, assessment and advice; and*
> *h. engage and cooperate, where appropriate, with international organisations,*
> *partners and other relevant stakeholders…*"

---

[16] See the ICAO Facilitation Panel working paper of September 2018 at https://www.icao.int/Meetings/FALP/Documents/FALP10-2018/FALP10.WP5.Single%20Window-Netherlands-Final.pdf . See also the Dutch presentation in this matter at https://www.icao.int/Meetings/FALP/Documents/FALP10-2018/WP5.Single%20Window%20for%20passenger%20Information.pdf

The Boe Declaration Action Plan[17] further elaborates these mechanisms in respect of Strategic Focus Area 4 (Transnational Crime) and Strategic Focus Area 6 (Creating an enabling environment for implementation including an appropriate coordination mechanism).

The language in both documents provides a clear indication that establishment and strengthening of regional coordination mechanisms which support the national security and sovereignty of members in response to these threats, is fully supported by PIF leaders.

2.3   API in the broader Border Management Context

Coordinated Border Management

Coordinated Border Management (CBM) is a fundamental development in management theory around migration and border management. Emerging from the World Bank and WCO [18], supported by ICAO and the International Organization for Migration (IOM), the value proposition lies in the fact that a properly coordinated approach shares the systems, resources and skills of agencies, stakeholders, countries and regions to manage ever increasing complexity and volumes more effectively and at reduced cost per traveller.

The CBM concept has been described via several different names, including "Collaborative Border Management" (a term used by the World Bank), and the Organisation for Security and Cooperation in Europe's term "Comprehensive Border Management". IOM also commonly uses the term "Integrated Border Management".[19]

CBM brings change to management structures within agencies, arrangements between agencies and carriers, and IT system or BMS design, all based upon principles of interoperability and

---

[17] See https://www.forumsec.org/wp-content/uploads/2019/10/BOE-document-Action-Plan.pdf

[18] See "Coordinated border management: from theory to practice" by Mariya Polner, World Customs Journal, 2011, Vol 5, No. 2, pages 49-64, http://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/coordinated-border-management.aspx; World Customs Organisation, Coordinated Border Management Compendium, 2015, available at http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/cbm-compendium.pdf?la=en; Tom Doyle, "The Future of Border Management", Chapter 2, World Bank – Border Management Modernisation, 2011, available at http://documents.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf ; McLinden, Gerard, "Collaborative border management : a new approach to an old problem", 2012, World Bank, available at http://documents.worldbank.org/curated/en/693361468331207794/Collaborative-border-management-a-new-approach-to-an-old-problem

[19] See "Coordinated border management: from theory to practice" by Mariya Polner, World Customs Journal, 2011, Vol 5, No. 2, pages 49-64, http://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/coordinated-border-management.aspx; World Customs Organisation, Coordinated Border Management Compendium, 2015, available at http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/cbm-compendium.pdf?la=en; Tom Doyle, "The Future of Border Management", Chapter 2, World Bank – Border Management Modernisation, 2011, available at http://documents.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf ; McLinden, Gerard, "Collaborative border management : a new approach to an old problem", 2012, World Bank, available at http://documents.worldbank.org/curated/en/693361468331207794/Collaborative-border-management-a-new-approach-to-an-old-problem.

information and burden-sharing within defined governance mechanisms. It recognises there is a multiplicity of agencies and stakeholders at the border, and instead of regarding this as a problem, treats it as an opportunity.

Properly implemented, CBM enhances the chances of early risk or threat identification, meaning scarce resources can be diverted to areas of need, with the vast majority of legitimate travellers and trade managed as "low risk" and accorded a "light touch" approach at the border or during related processing.
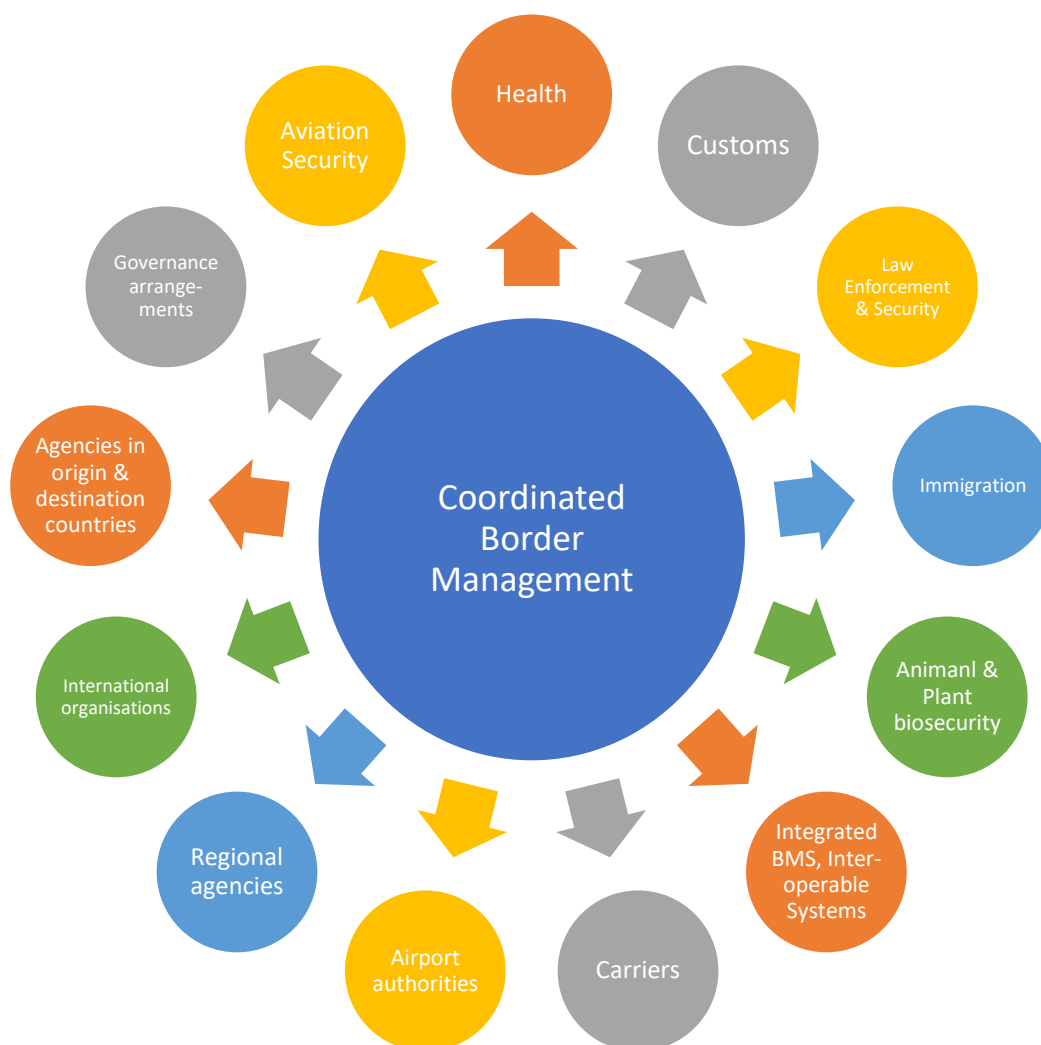

Figure 4: CBM stakeholder engagement

The Pacific and Integrated Border Management Systems

The introduction of global standards around API and information sharing, along with the development of border management principles have expanded the expectations around border

management systems. The data exchange standards and pre-clearance methodologies set out in this paper generally (but not exclusively) rely upon countries having a BMS that is interoperable with them, and represent a capability which should be considered in any future BMS procurements, upgrades, or replacements.

A caution with BMS arrangements in the Pacific is that they should not seek to over-complicate the solution, or be too expensive to procure and operate. Business and technical requirements need to be understood and balanced against budgets and agency resources. For example, API integration need not include the more expensive and complex iAPI, where the simpler batch API will suffice.

Passenger Data Single Window (PDSW) arrangements for API and even PNR also need not be overly complicated, and depending upon arrangements with carriers, may be little more than a single email address which auto-forwards data to designated agencies for upload by a designated team into an assessment system, a BMS, or both.

Whilst not essential, implementation of API is further augmented by the implementation of ETA and online e-Visa capabilities within a BMS environment. This provides a means to check the identity and intent of travellers at least once before they check-in, and then again via API as they check-in.

When considering the deployment or upgrade of BMS systems, it is clear from ICAO's work in this area that they should not be regarded as a standalone operation. Whilst the BMS in operation at the primary line does not necessarily need to be a part of the same system which manages, for example, visas or national passports, or even alerts, it is critical that these databases are interoperable so that data within them can be cross-referenced and verified in real-time by officers performing each of these functions.

Immigration agencies should seek to ensure they value-add to BMS deployment and operation by advocating for, and where they "own" a system, implementing the principles of interoperable and interconnected systems, delivering **Integrated Border Management System** (IBMS) services across Government. This should form a core part of thinking in any systems upgrade or procurement exercise.

Recommendation 5: Consistent with the principles of CBM and UNSCRs, consideration should be given to improving PIDC members' border management through:

- the direct acquisition of API systems capability by PIDC members; or
- the central negotiation and procurement of API systems capability by an organisation, such as PIDC, on behalf of all interested members.

2.4   Technological considerations & practical applications

Data Standards

As discussed above in this report, key principles of API are that the data is:

- Electronic, not hardcopy, and
- In a standardised format

This allows the data to be subject to computerised data matching, checking and analysis, which in many cases can be automated.

Relevant standards recognised by ICAO, WCO, IATA and carriers are:

- API – UN/EDIFACT PAXLST
- iAPI responses - CUSRES
- PNR - PNRGOV[20]

There has been further development of XML format data exchange methodologies such as ebMS, with standards being released for XML PNRGOV data transmission[21]. This has enabled web-based collection and transmission of data to and from Government, separate from or in addition to more traditional methods listed above, which rely on networks such as that run by SITA and ARINC. XML data exchange mechanisms have also been established by some individual countries for the use of carriers.

XLS format spreadsheets and file upload portals have also been established for small craft, yachts, and private aircraft, which will often not have access to the more sophisticated modes of API transmission above. A notable example is that of the CARICOM Implementation Agency for Crime and Security (IMPACS) Advance Passenger Information System (APIS) portal.[22] PNG Immigration also operated a similar model for the import of cruise ship manifests within their BMS until recent years, with standardised Excel (XLS) spreadsheet formats utilised to capture data of those aboard emailed by operators to a centralised email address.

API transmission from carriers to border control agencies is subject to a standardised set of data fields, agreed to by ICAO, WCO and IATA[23]. These are

1. Data relating to the Flight (Header Data)
2. Data relating to each individual passenger (Item Data) which may include:
   a) Core Data Elements as may be found in the Machine-Readable Zone of the Official Travel Document
   b) Additional data as available in Airline systems
   c) Additional data not normally found in Airline systems and which must be collected by, or on behalf of the Airline.

Recommendation 6: Members should consider adoption of the standard set of API data fields used for transmission from carriers to border control agencies, as defined by ICAO, WCO and IATA, as prescribed in the *Draft Regulations* at **Annex 3, Schedule 1** of this report.

---

[20] See the ICAO Guidelines at
https://www.icao.int/security/fal/sitepages/api%20guidelines%20and%20pnr%20reporting%20standards.aspx
[21] See IATA's guidance on this at https://www.iata.org/en/publications/api-pnr-toolkit/#tab-3
[22] See https://caricomeapis.org/
[23] See Chapter 8 of the WCO/IATA/ICAO API Guidelines at
https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf

PNR data is by definition more nebulous, and whilst it is subject to a transmission standard (PNRGOV) and data field definition in ICAO Document 9944[24], the data collected and held in PNR records varies significantly from airline to airline, and also between individual travellers depending upon their circumstances. It is also dynamic, changing as a booking varies or changes, or payment is made and tickets are issued, and check-in occurs.

Where it is required, PNR is often required to be "pushed" to Governments, to a maximum of 5 times:

        1) -72hrs,

        2) -24hrs,

        3) -2hrs

        4) -1hrs

        5) Wheels Up

The latter often includes both PNR and API data, which is an efficient means of conveying both data sets.

The complication for any Government considering initial API implementation is that, as discussed in Chapter 2 above, EU Data Protection requirements are very stringent, and may restrict the availability of PNR data until bilateral agreements are signed between the EU and individual requesting Governments. This restriction does not apply to API data which is another reason why PNR implementation should only be considered after API data transmission, reception and analysis has been successfully achieved.

Data assessment and the requirement for a BMS

As will be further documented in Chapter 4 below, it is not absolutely essential that a country or territory operates a BMS in order to receive API data, and carry out assessment of passengers with that data. For example, assessment tools, such as Interpol's i24/7 & Stolen and Lost Travel Document database (SLTD) systems, WCO's GTAS, US CBP's ATS-G and UNOCT's goTravel[25] are separate from a national BMS but still allow a PICT to check API data against its internally generated profiles and indices. However, integration with a national BMS also allows for checking against immigration alert lists, as well as validation of national visa and passport data, maximising the value gained from the exercise.

---

[24] See ICAO's guidance, including Document 9944 at
https://www.icao.int/Security/FAL/ANNEX9/Pages/Publications.aspx
[25] See links to these systems as follows: Interpol SDLTD - https://www.interpol.int/en/How-we-work/Databases/Stolen-and-Lost-Travel-Documents-database , GTAS - https://us-cbp.github.io/GTAS/ ,
ATS-G - https://www.cbp.gov/frontline/cbp-national-targeting-center and goTravel -
https://www.un.org/cttravel/goTravel

Likewise, it is not essential that these other analysis tools are utilised, as checking the data against a BMS alone may be regarded as, at least initially, sufficient to ensure known travellers of concern who are already listed in BMS alerts are identified.

Rules and profile-based assessment tools, such as those listed above, bring additional and highly valuable analytical capability, generally well beyond that of the BMS alone. Use of these is free, and there is generally considerable support offered by the provider in terms of installation and integration with airline systems and BMS.

- **Interpol's databases** can be accessed via its online i24/7 system, or in offline mode via its MIND system. This includes the SLTD, and its nominal databases of persons wanted internationally. API data can be run against these databases automatically where a connection is established to the BMS or the analytical system which performs the analysis of the data.

- **ATS-G** is the US Customs & Border Protection's (CBP) "automated targeting system-global". ATS-G is similar to the software used at the Office of Field Operations (OFO) National Targeting Centre and evolved from decades of experience designing and operating passenger and cargo targeting systems. The software can vastly improve how travellers flying in and out of a country are vetted. It is offered with a free license, but does involve data sharing with US CBP.

- **GTAS** – also developed by US CBP, but under the leadership of WCO, GTAS permits foreign countries to independently perform vetting activities without the collaboration or information sharing with the US involved with ATS-G. Operating in 3 countries, with others in the process of installation, GTAS is free and designed for rapid use. The software is easily downloaded from a special CBP website and ready to use. It can also improve an existing vetting system because the coding allows nations to customize the software or just download the portions that meet their needs. GTAS is comparable to ATS-G because GTAS also automatically evaluates passenger manifests in real time to identify suspicious travellers or crewmembers who may pose a national security risk, justifying a closer assessment. Using GTAS, governments can screen suspects before they enter or leave that nation.

- **goTravel** –is a United Nations-owned software solution derived from the Travel Information Portal (TRIP), developed by The Netherlands, and installed under that version in 10 countries. Free to use, goTravel can

  o Perform as a single window receiving API/PNR data from carriers, accepting multiple data transfer standards
  o Allow configuration of rule-based risk indicators and watchlists, and list the records that are matching against those rules
  o Perform an assessment of passengers prior to their scheduled arrival/departure (matching with risk indicators, watchlists and Interpol databases)
  o Manually query API/PNR data for the purpose of helping competent authorities during ongoing investigations
  o Automatically notify competent authorities when goTravel identifies passenger data requiring further examination

- o Enable verification of PNR/API data retrieval and data quality of connected air carriers
- o Enable analysts to reveal relationships between objects such as passengers, phone numbers, credit cards, etc. and visualize connections on graphs
- o Use network analysis to identify formally unknown relationships

The Interpol, goTravel and GTAS and systems are ideally suited to a deployment in the Pacific as they are internationally recognised and supported, free of license fees, have a track record of successful integration with other national systems, follow international data transmission standards, and do not involve data sharing with providers. At this stage they do not support iAPI.

Data import - Systems Integration

Where a BMS exists, some form of integration with API is highly recommended. This may take the form of simple functionality allowing the upload of API data received by email in spreadsheet form (batch) into a BMS to create an "expected arrivals" manifest for a flight or vessel, which can then be run against alerts, visas, and passports data prior to arrival.

For busier ports, some form of semi- or fully-automated upload into a BMS may be considered, using a feed from SITA or ARINC, or via a custom-built XML portal, however this will come at a cost, which must be balanced against the expected benefit, and analysis as to whether the passenger facilitation and security outcomes can still be met through having well-trained staff upload batches of API in a timely fashion as they arrive.

Similarly, there is a need to integrate API data feeds, or at least import the data into the other assessment tools listed above. Whilst assistance is provided in each case, the complexity and ongoing maintenance may still prove daunting to smaller agencies and PICTs. This may be overcome where a regional approach is taken such as that suggested in this report.

Recommendation 7: It is highly recommended that some form of API integration be adopted by those PIDC members which have a BMS.

Security and Reliability, Budget & Ongoing viability

Given the sensitivity of API and PNR data, similar to that of a BMS, it is essential that transmission, reception, storage and analysis of API (and PNR) data is achieved reliably, and securely. Receiving agencies should ensure relevant systems and hardware are up-to-date, and secured behind appropriate physical and software safeguards and controls.

Firewalls, VPN arrangements, and anti-malware must be properly maintained, and where Cloud hosting is considered, should be with top-tier providers such as Amazon AWS, Microsoft Azure, or Google Cloud. Should any other provider be considered, they should meet the security, service-level agreement, and up-time standards of these providers.

Locally hosted servers and communications equipment should be of recognised brand names, and hardware refreshed as it approaches end of warranty in every case.

This requires that sufficient annual budget is earmarked specifically for these purposes, planned for and approved well in advance of initial deployment, as otherwise the viability of systems to support API will become imperilled in only a few years.

A regional solution, where these burdens are shared among several agencies or PICTs may address some of the genuine concerns which arise with seeking implement this technology individually.

Recommendation 8: Border control agencies that receive data should ensure relevant systems and hardware are up-to-date, and secured behind appropriate physical and software safeguards and controls.

2.4   Domestic Legal & Governance Requirements

The Immigration Act is widely considered to be one of the few key pieces of government legislation which directly impacts and supports the 3 main pillars of good and effective government – national security, economic growth and prosperity, and social harmony and well-being. In the context of the effective implementation and operation of API, it should provide the legal authority for the collection of information (including biometric information) about people arriving and departing and also provide the authority for the retrieval and sharing of information with other domestic agencies and with prescribed overseas agencies and carriers, in accordance with national inter-agency and international bi-lateral and multi-lateral agreements.

Appropriate safeguards about what, how and to whom specific information can be shared should be prescribed in the Regulations which underpin the Immigration Act or some other form of legislative instrument. The presence of the requisite Heads of Power in the Immigration Act and regulatory controls over the sharing and use of information in secondary legislation (Regulations) is critical to any prospective adoption of API-type arrangements. Without them, information activities can be seen as unfair, a breach of a traveller's privacy and hence open to legal challenge. As detailed in **Annex 3**, this issue has emerged as a major concern for a range of government and non-government stakeholders in several PIDC members across both the North and South Pacific.

In parts of the Pacific, the policies and enabling legislation for the control of people movement and border protection date back to colonial times. It is sometimes fragmented and administered by different portfolios, most likely reflecting the way that legislation and public administration have developed historically. In some instances, it includes cross-references to other legislation, and mandates authority and accountability for the exercise of certain powers on institutions and positions which no longer exist. In an increasingly joined-up and litigious world, these pose serious legal and border management risks for the governments concerned as well as creating rigidity and deterring innovation in border management practices.

In order to assess the degree of legislative capability to support the introduction of API in the Pacific, CBS has examined the current Immigration legislation of the 18 PIDC members to determine whether

there is sufficient authority for the sharing of information, as this is at the heart of any API/PNR/APP system. The results of this examination are tabulated at **Annex 1** to this report.

They show that all of the PIDC members would require amendments to their Immigration legislation in order to lawfully share information about people movement with other national and international agencies and carriers. The possible exceptions are Samoa, which passed a new Immigration Act in 2020 and is currently in the process of developing a new suite of supporting Immigration Regulations, and the Cook Islands which is considering an advanced draft Immigration Bill and Regulations. Although it should be noted that insufficient information was available to CBS about the legislation applying in the current and former French Territories to form a firm opinion, from the information that is to hand, it would appear that legislative amendments would be required.

CBS is aware that over the past decade several PIDC members have completed reviews of their immigration and visa policies and underpinning legislation, sponsored by PIDC and/or the African, Caribbean and Pacific Group of States (ACP)-EU. These include: the RMI, Samoa, FSM, PNG, Tonga, Solomon's and Tuvalu. As part of these reviews, CBS consultants have had the opportunity to participate in numerous rounds of consultations on immigration arrangements with stakeholders from a wide range of PICTs.

One of the main themes to emerge from these consultations is that stakeholders are generally very supportive of better information sharing between agencies but some have highlighted the fact that such sharing may require consideration of relevant domestic laws and policies pertaining to informed consent and privacy. A detailed examination of each individual PICT's privacy legislation is beyond the scope of this paper but, suffice it to say, where a country has privacy laws, these must be considered (and reviewed as necessary) in conjunction with any proposed changes to Immigration legislation to enable the lawful sharing of information, both domestically and internationally.

To assist this process, draft model legislative provisions have been developed for the consideration of PIDC members, located at **Annex 2**. The wording of these is not intended to be prescriptive and it is, of course, open to PIDC members to choose different terminology, customised to meet their specific needs, policy and processing environment, to achieve the same outcomes.

Key components of these model provisions, which have been informed by both regional experience and that of the Caribbean regional body, CARICOM, include:

- Specific heads of power and offence provisions in the Act relating to API, with much of the detail in more easily amended and updated Regulations
- The capability to have a designated national body or authority receive and assess API data, which may or may not be separate from Immigration as desired, such as a national border security fusion centre, a Transnational Crime Unit (TCU), or similar
- The capability to engage a Regional Organisation, such as PIDC, to receive and on behalf of members States, analyse API data and transmit both data and results to member States

- Maintenance of sovereignty of decision-making around border clearances.

Recommendation 9: It is highly recommended that renewed emphasis be placed on the review and modernisation of PIDC members' Immigration legislation order to create an environment conducive to the introduction of API and information sharing more broadly, consistent with the principles of CBM.

---

3. The Current Situation in the Pacific

Based upon available data and research of the authors, it is estimated that in 2019, there were the following volumes of travel to and from PICTs:

- Air: 5 million[26]
- Sea: 2 million[27]

These figures include both arrivals and departures, and include citizen and non-citizen travel, and for all purposes including cruise ships, crew, work, resident, visitor and tourist.

Implementation of API is uncommon among PICTs, with most relying upon hardcopy flight and shipping manifests, which are often provided shortly before arrival, or even afterwards.

Cook Islands Customs receives API data via the New Zealand SITA data transmission arrangement; however, this is an exception, and as is the case elsewhere in the Pacific Islands, there is no analytical capability associated with passenger data beyond manual checking against BMS holdings (unless New Zealand does this on behalf of the Cook Islands). SITA and ARINC data feeds are generally not available to PICTs, and where electronic manifests are provided at all (such as air carrier data to Fiji Customs and cruise ship data to PNG Immigration or maritime movements to Customs services), this is by email and may not be standardised.

Whilst most PICTs have some form of BMS, most of these systems do not have API upload or assessment capability, even at a basic level such as batch uploads of spreadsheets, creating a list of expected movements for arriving craft, and checking against alert lists.

Cook Islands, Kiribati, Nauru, Niue, Tonga and Tuvalu are receiving the UNCTAD Passenger Processing Module (ASYPX) system, which, whilst still under development, is understood to have batch API and Interpol SLTD functionality included among its specifications. IOM's Migration Data Management, Intelligence and Risk Analysis System (MIDAS), installed in the Marshall Islands, also has batch API & Interpol functionality, although this is not yet implemented as the domestic legislation does not yet cater for API. The MERIT BMS, installed in Samoa does not have this functionality, although the PNG

---

[26] Estimate based upon World Bank figures, and adding known numbers from countries omitted from the World Bank report, such as Cook Islands & PNG. The figures do not include Australia, New Zealand, or the US. See https://data.worldbank.org/indicator/IS.AIR.PSGR?locations=S2 and https://data.worldbank.org/indicator/IS.AIR.PSGR

[27] Includes Australia and New Zealand. Estimate based upon SPTO and Cruise Industry reporting at https://southpacificislands.travel/rtrc/ , https://cruising.org/-/media/research-updates/research/clia-2019-state-of-the-industry-presentation-(1).ashx and Statista Reporting at https://www.statista.com/statistics/287111/cruise-passengers-by-source-country/

version (the most up-to-date) has Interpol connectivity and could be modified relatively easily to include batch API capability. Fiji's Informatics IBMS has Interpol functionality, and could also be upgraded to accommodate batch API.

Linkages with Interpol indices such as SLTD are also the exception, with only Fiji and PNG known to have an automated connection to their BMS as detailed above. None perform checking of API data against Interpol systems, except on a manual individual basis where circumstances may dictate.

Perceived obstacles include the need to procure, upgrade or replace a BMS, the need to make arrangements with carriers to obtain API data, the cost of data feeds from SITA/ARINC or creating API data connections or websites for uploads, complexity of systems integration, and lack of enabling legislation. Human resource and capability constraints as well as budgetary constraints are acknowledged around the region, with agencies ranging in size from 4 to around 180 staff (the latter seen only in PNG and Fiji).

In order to derive the most value from API data, it should ideally be received and analysed prior to an aircraft departing the last port of embarkation, or in the case of maritime movements, well prior to the arrival of a vessel. This allows the possibility, at least for air movements, that a traveller could be prevented from boarding or be offloaded prior to take-off, vastly improving border security outcomes in extreme cases. In all other cases, those aboard aircraft and vessels will ideally be profiled into "low risk" or "higher risk" before arrival.

Some flights into the region emanate from more distant ports in Asia and the Americas, meaning that in order to achieve these outcomes, assessments may need to be undertaken outside normal office business hours, and for many PICTS, may require a 24/7 operation, preferably involving key border agencies such as Immigration, Customs, and Biosecurity as well as possibly Police.

Whilst proper assessment of API data may bring greater efficiencies to border operations, allowing redeployment of some staff, the establishment of individual, national a 24/7 operations would likely impose a significant burden on even the largest agencies within PICTs. Joint Border assessment teams exist in some PICTs such as Fiji, however those encountered elsewhere are generally reactive, compliance-based teams rather than focused on pre-arrival assessments, and do not operate on a 24/7 basis.

4. Possible regional approaches

4.1   The CARICOM Example

CARICOM is the Caribbean Community, a regional forum which is in many ways similar to the PIF.

The CARICOM IMPACS -Joint Regional Communications Centre (JRCC) is one of two (2) Sub-Agencies of CARICOM IMPACS, the other being the Regional Intelligence Fusion Centre, based in Trinidad.

Both sub-agencies were formed for the purpose of supporting the Regional Security Strategy for International Cricket Council Cricket World Cup 2007 (ICC CWC 2007).

As a result of these sub-agencies' successes, Heads of Government at its Eighteenth Inter-Sessional Meeting in St. Vincent & The Grenadines in February 2007 endorsed a proposal for the permanent establishment of the two sub-agencies.[28]

The JRCC manages two systems:

- CARICOM Electronic Advanced Passenger Information System (eAPIS)
- CARICOM Electronic Advance Cargo Information (eACIS)

The APIS system is the focus of this report, however it is noteworthy that the JRCC jointly assesses the movements of people and cargo within the region.

The JRCC APIS has been established with a legislative mandate in each of the 17 participating countries to, on their behalf, receive and analyse API data. Model legislation, developed by the JRCC has been communicated with members, who have been able to incorporate key elements within their domestic legislation to enable and authorise this initiative. This model legislation has informed the drafting of the suggested legislative amendments for PICTS, at **Annex 2**.

The JRCC sub agency is located in Barbados and is staffed by a combination of both contracted and seconded staff. Many are of a law-enforcement, borders, or intelligence background, and are recruited from among member States, who fund the salaries of their own staff, which is supplemented by the JRCC to support the relocation to Barbados, such as housing allowances etc. The US CBP service also has one officer seconded to the JRCC to provide liaison and support.

The JRCC is mainly responsible for the operations and management of the APIS, which screens approximately forty (40) Million passengers annually, specifically those entering, and travelling within the CARICOM Region by air and sea ports.

The JRCC currently receives and analyses only API data, not PNR, and does not operate any form of iAPI.

It currently has a US$9 million budget, and has 16 staff operating 24/7 on 2 x 12-hour shifts conducting the analysis of both travellers and cargo.

---

[28] Adapted from the JRCC website at https://caricomimpacs.org/

Figure 5: Border protection process **supplied by CARICOM JRCC**

As can be seen from the diagrams above and below, the JRCC receives API data from air and sea carriers, as well as operators of small craft and private aircraft via the following means:

- SITA & ARINC feeds (standard Type-B)
- The eAPIS website (XLS, XML & UN-EDIFACT)
- Customised web-feeds

The SITA and ARINC data feeds are basic Type B feeds, which are sufficient for the effective transmission of API, and are not comparable to the regional offering detailed by SITA in section 4.2 below. The JRCC report that operating costs of these are US$9000 to US$9600 per annum each, and note that both networks charge differently depending upon passenger volumes, and that these reflect the value gained by having a larger joint volume, i.e., less cost per passenger by having one connection from each rather than one connection per country.

The JRCC technical team lead expressed the opinion that whilst both SITA and ARINC were able to offer value-added services such as analysis tools and links to Interpol systems (for example), these were expensive compared to setting up and operating these independently via a regional body such as the JRCC.

Data is subject to several concurrent analyses, utilising the US CBP ATS-G system, the UNOCT goTravel system, and an in-house analytical tool.

Data is also concurrently sent to the receiving country's designated agency, via a secure VPN link, so that domestic analysis may also be conducted, such as against the national BMS.
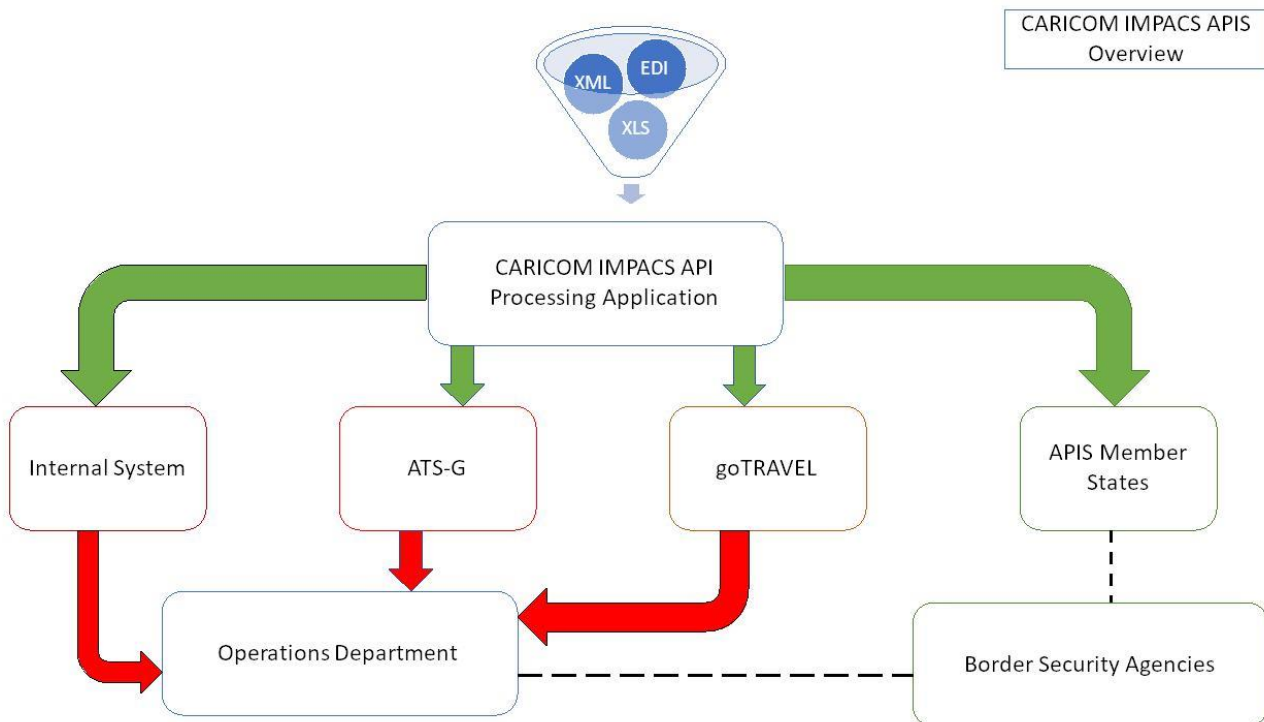
Figure 6: CARICOM APIS supplied by CARICOM JRCC

The results of JRCC analysis are transmitted to the receiving country, which along with their own analysis, uses this to decide the approach to incoming travellers in each case.

Decision-making remains at the national level, but as can be seen, is enhanced by the combined resources of member States in jointly funding, staffing, and operating the central analysis centre.

National API data is not shared with other member States, apart from the linkage with the ATSDS-G system and the US CBP service. This ensures privacy of data among members, and embeds a need-to-know culture.

Funding is currently via donor support, predominantly from the US, and also via member contributions. No passenger levy or tax has been implemented to fund the operation, although it has been proposed several times but has so far failed to gain sufficient support among the membership.

Membership is similar to that of PIDC, with the largest State (Trinidad & Tobago) having a population of 10 million, and the smallest (Montserrat) having a population of 5000. Immigration services are also of a similar varying range of size and capability, and legislation is often similar in that it may be significantly influenced by former colonial powers (such as the British Common-law system), and when the JRCC was proposed, required amendment.

It is clear that, presented with a major event in the Cricket World Cup in 2007, CARICOM members recognised they were unlikely to be able to manage the collective security analysis needs arising

from it. Proper reception and vetting of API data required an expertise which did not exist in all countries. The JRCC was born with donor support, backed by a regional political will to combine resources in a manner compatible with CBM.

Recommendation 10: CBS suggests that the CARICOM JRCC may be a viable model upon which to base a collaborative Pacific regional API collaborative arrangement.

4.2   The SITA example

SITA is, along with ARINC, one of the two major aviation industry network and communications providers. Both provide industry-standard API and PNR data feeds between carriers and Governments, as well as other airlines systems including DCS and reservation systems, along with integration between all elements. Both can accommodate iAPI, and in the case of SITA, ETA solutions as well. Both also provide biometric-enabled border control systems such as e-gates.

CBS approached SITA given its presence in the Pacific and regional history working to initially develop ETA and API capability from the 1990s, in order to determine what they might offer a region in addition to basic, direct standard data feeds already described (such as the Type-B messaging standard).[29]

SITA has developed a combined API/PNR gateway[30], which can accept standard format data from carriers (air and sea) via their network, direct from carriers via XML, via emailed Excel (XLS) batches, or via a web-portal designed for the purpose.

The system receives manifest (API) data, booking PNR data, and check-in (DCS) data, and combines this into a single message format as required by the recipient Government, which is then available via a secure single-window facility accessible by authorised users of relevant recipient country agencies. The data is checked for timeliness, completeness, and accuracy, with artificial intelligence and machine-learning capabilities able to detect accidental and deliberate data errors, and where possible, correct these.

Data can be downloaded or automatically transmitted to integrated systems, such as a BMS and/or analysis tools such as GTAS. SITA is able to carry out these integrations, and is also able to enable checking of the data against INTERPOL indices via its FIND (i24/7) system.

The system is compliant with EU privacy laws (the GDPR) around security and data retention, with data purged from the SITA-side of the system once transmission to the recipient Government is complete.

Interestingly, the gateway is, when combined with stand-alone analysis tools such as GTAS, not reliant on a Border Management System. As discussed elsewhere in this report, checking API data against BMSD holdings is clearly preferred, but in this case where this does not exist, the data

---

[29] This should not be seen as any specific endorsement by the authors of SITA, and it is recognised that ARINC is likely to be able to deliver similar solutions, as may other similar aviation industry providers.

[30] Refer to https://www.sita.aero/solutions/sita-at-borders/border-management/sita-api-pnr-gateway/

from the gateway can be run against these other analysis tools and the INTERPOL indices, which still adds significant value.

Another clear advantage of the SITA gateway is that relationships with carriers is fully outsourced to SITA, reducing the governance and liaison burden upon recipient Governments.

In the interim report on this topic, submitted to PIDC on 23 June 2021, the authors indicated that SITA was yet to finalise their costings and define the full offering to regional partners; however, it was expected that the transaction unit cost would be less than US$1 per traveller.

A more detailed proposal has now been received, which has been included at **Annex 5** of this report. The SITA offering is based upon the premise that a regional community model is adopted for countries willing to participate. The proposal does not constitute a formal commercial offer, with final pricing being subject to the outcome of negotiations between interested parties (possibly also including PIDC if members request this), and the approval of SITA's Business Approval Board.

Importantly, SITA's modelling of costs is at Part 6, pages 13-16 of their document (**Annex 5** of this report). This proposal brings added value, but also higher costs than those which can be expected should simpler, more basic industry standard data feeds be sought (such as Type-B). These costs are detailed in the CARICOM example above.

SITA confirm that they are a member of the IATA Clearing House[31], a service operated by airlines via IATA which would (where authorised by legislation or other similar mandate) enable them to levy any such cost onto airline tickets. This would see a very small additional cost borne by individual travellers, which would in turn make the gateway self-funding once established and fully operational.

The issue with a solution of this kind is that costs of analysis (staffing etc) are not part of the costs covered by this model. Similarly, local systems integration costs are not included, and the funding model as it stands, would serve to cover only the SITA system costs. A possible solution to this is explored in section 4.4 below, where a joint assessment centre is proposed to share the cost and resource burden. As will be seen, this joint regional solution is not contingent upon also taking up an offer such as that proposed by SITA at **Annex 5**.

Recommendation 11: PIDC should consider the implications of SITA's model which serve to highlight the potential for cost-effective "regional" service offerings to Governments facing significant resourcing and capability constraints.

4.3   Possible Pacific Models

The individual national approach

It is open to PICTs to implement API connectivity and assessment capability on an individual basis. Indeed, there will always remain a national, sovereign decision around which non-citizens may be

---

[31] See https://www.iata.org/en/services/finance/clearinghouse/

permitted to enter and/or remain in each PICT, meaning at least some checking and assessment of API within each PICT is likely to be required. This should not change whichever model is chosen. However, the complexity and cost, as well as the burden of implementation and maintenance is likely to be greater where the individual model is chosen.

System integration and/or change may be required to allow API data to be uploaded into a BMS for checking, validation, and creation of expected movements lists, even where this is at its most basic via uploading of Excel (XLS) files. The costs of this for each country will vary depending upon the BMS in place, however it can be expected that amendments to a fairly capable BMS to enable manual batch API data import and checking, along with INTERPOL connectivity (where these do not already exist) would cost anywhere from US$25,000 to US$150,000.

These costs will not be incurred, or will be minimal where the BMS already accommodates this functionality. Those PICTs known to have this capability are detailed in Chapter 3 above.

Additional cost and complexity come with establishing and operating the SITA and/or ARINC data feeds, the creation of individual portals to allow direct XML data connections with carriers, and the establishment of alternative mechanisms to allow ad-hoc API data transmission from small craft and private aircraft, such as web-portals and/or email facilities. MoUs would need to be established by each PICT with carriers. SITA and ARINC data feeds to not need to involve the additional service and cost of the SITA regional offering detailed in section 4.2 above and **Annex 5**, and can follow the industry standard and less expensive Type B messaging format, however even this basic data feed will still incur a cost beyond many individual PICT Immigration agencies, and involve sometimes complex systems integration.

The addition of even free API assessment tools such as GTAS or goTravel will also require some systems support, as well as even basic integration with incoming data feeds. More complex deployments could include integration with BMS and other systems operated by other border agencies. This will bring costs, and a need for ongoing expertise and technical support.

Pacific Independent eAPIS Functional Diagram
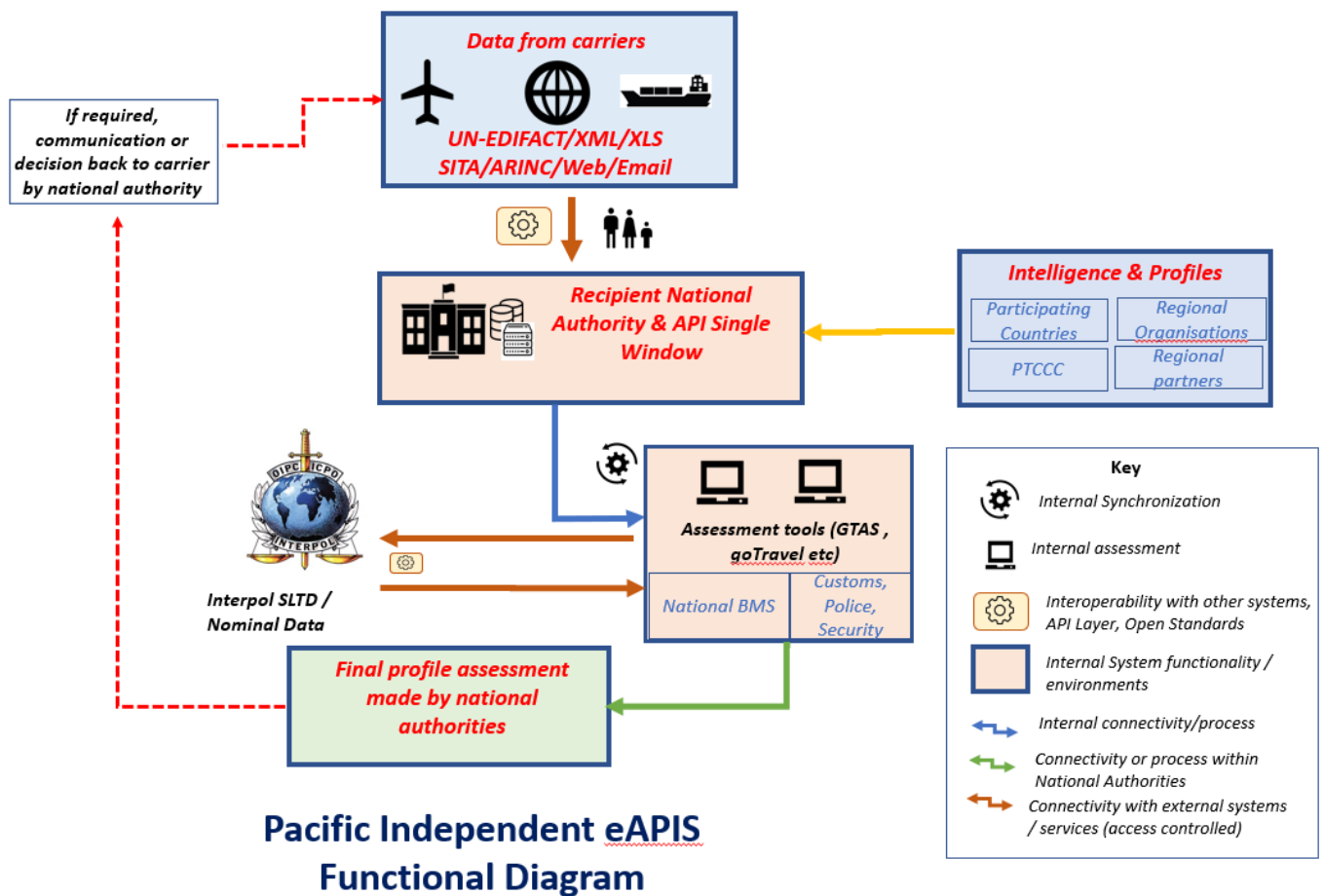
Figure 7: Possible eAPIS model for singe country

Replicating this process, as depicted in the diagram above, across each of the PIDC members would prove complex and, taking the costs of basic data feeds experienced by the CARICOM JRCC, which amount to US$18,000 as a guide, these costs would need to be borne by each member.

As is mentioned elsewhere in this report, deriving maximum benefit from API requires that the data is assessed as soon as it is received, which is in the 30-40 minutes prior to the actual take-off of the aircraft from the port of embarkation in the case of flights. Even for smaller PICTs with fewer flights and cruise ship arrivals, this will often require out-of-hours, and even a 24/7 staff presence to conduct the assessments and flag travellers of concern prior to arrival. This would come at a significant cost to even the larger PICTs, and for busy airports and ports, may require several staff on several shifts, 24/7/365.

These costs, if borne directly by the agency concerned, would pose a significant hurdle, as would the technical expertise necessary for systems configuration, integration, and support.

Recommendation 12: It is recommended that, while it is open to PIDC members to implement API connectivity and assessment on an individual basis, the potential benefit of economies of scale will not be realised meaning that the complexity and costs are likely to be greater because at least some checking and assessment of API within each PIDC member country will be required.

A Regional Approach

A regional approach similar to that taken by CARICOM is enticing in the Pacific as it stands to deliver the required capability at a fraction of the cost to each participant, both financial and human.
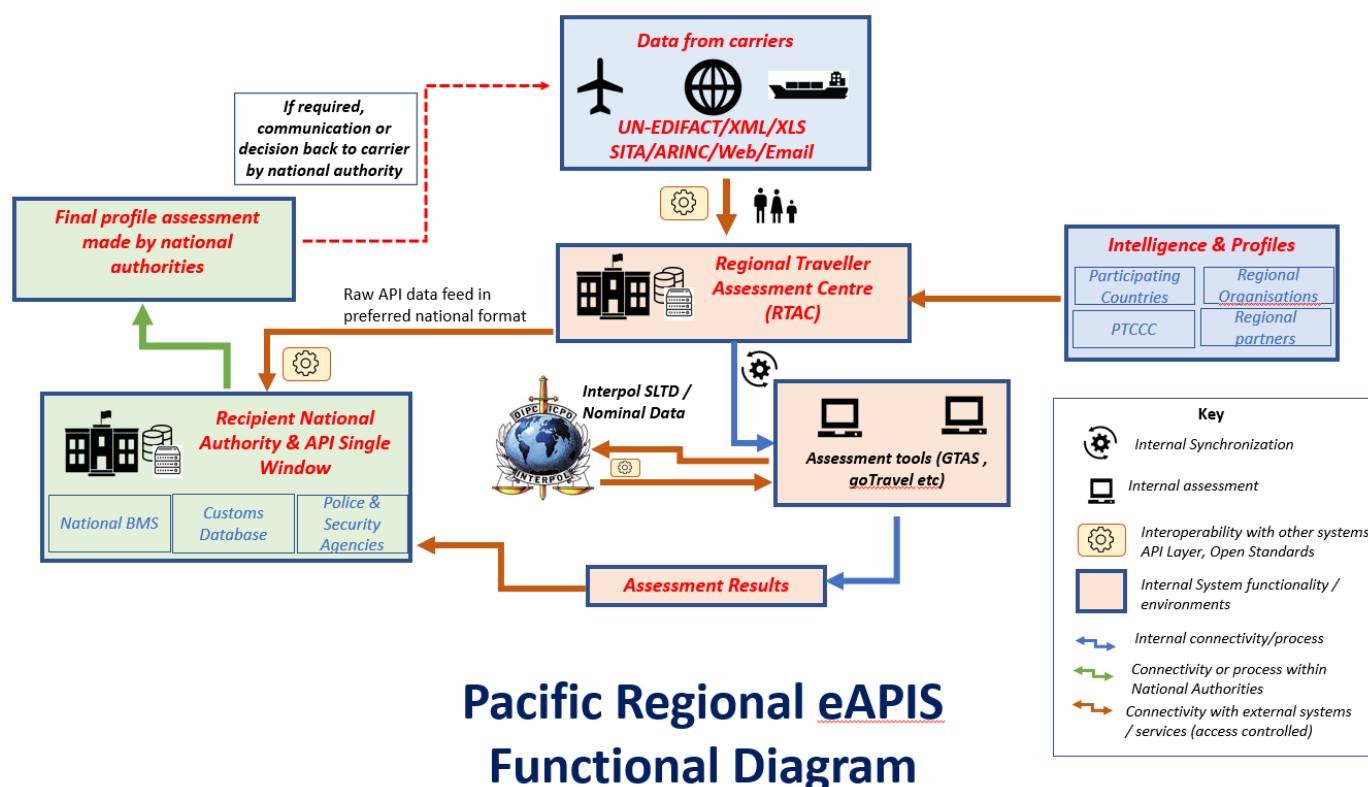
Figure 8: Possible Regional eAPIS model

As highlighted in the SITA example in section 4.2, a regional approach allows smaller PICTs which either do not have a BMS, or do not have a BMS which is API capable, to still derive benefit from API data. The possible regional approach, outlined above, envisages API data being received by a Regional Traveller Assessment Centre (RTAC) or however named, which would share the cost and technical burden associated with this among participants. Instead of each paying a fixed cost of (at least) US$18,000 per annum to SITA and ARINC together, and running other data collection facilities individually, this would be operated by the RTAC.

API data would be simultaneously transmitted to the receiving country as well as to an assessment facility operated by the RTAC, utilising one data feed from each source, saving costs. This could be a physical co-located office environment, or a virtual centre with participating agencies logging in remotely via secure VPN connection.

Assessment would take place within the RTAC, utilising INTERPOL systems as well as properly configured GTAS and/or goTravel systems which would be populated with assessment "rules" and any watchlists supplied by or agreed to by participating PICTs. UN terrorist watchlists, data

available on public sex-offender databases, and known trans-national criminals could be added to lists and profiles held by the Centre.

The value of API assessments is maximised where this is carried out in real-time, on a 24/7 basis. This is likely to prove challenging even for larger PICTs, thus the RTAC should be established and funded to enable this to occur centrally, as a service for participating PICTs.

This would not, however, take away from the ability of PICTs to also carry out their own assessment against national BMS and other databases, or impinge upon the ultimate sovereignty of each. The RTAC would not need access to national BMS or other border security data (although this could be accommodated if it was desired), and the decisions around treatment of travellers following assessment of API data would remain with national authorities.

Whilst there may remain costs to upgrade existing BMS or other systems to accommodate domestic API data upload and assessment in addition to that of the RTAC, costs are still significantly reduced overall, and depending upon the cost-recovery model pursued by participating countries, could conceivable be met by the budget of the RTAC.

Interpol systems integration could be accommodated via a law-enforcement agency agreement with the RTAC, which should be so designated by participating members, perhaps via the Pacific Islands Chiefs of Police (PICP). Intelligence shared by partners such as the Pacific Transnational Crime Coordination Centre (PTCCC) could value-add the work of the RTAC, which may ultimately be able to feed results or intelligence back where agree to participants, subject to clear governance mechanisms.

Systems may be physically housed with the RTAC, or should it be felt that this is too burdensome, part or all may be hosted with an appropriately secure cloud provider, such as Microsoft Azure, Amazon AWS, or Google Cloud. It is known that these operate classified as well as unclassified cloud services, which are likely to meet the security needs of participants.

Recommendation 13: A regional approach to API would allow smaller PIDC member states which either do not have a BMS, or do not have a BMS which is API capable, to still derive benefit from API data.

Recommendation 14: PIDC members should note that adoption of a regional approach to API would not diminish or absolve PIDC members from their ability and responsibility to also carry out their own assessments against national BMS and other databases, or impinge upon the ultimate sovereignty of members and their data.

Hosting a Regional Traveller Assessment Centre (RTAC)

Should a regional approach be taken by members, the question arises as to where and by what means this could be properly and lawfully hosted.

Possibilities include private companies, or having a single country hosting the service for all members, however neither of these is likely to satisfy security or sovereignty requirements of the

majority of members. Ultimately, as it involves assessment of sensitive traveller data against even more sensitive profiles developed to detect travellers of concern in the region, a body which is under the direct control of and answering to member States is optimal.

The example of CARICOM IMPACS JRCC is instructive, in that a regional organisation with its own legal status, controlled by its member States, operates the JRCC eAPIS.

Whilst it is by no means the only regional organisation in the Pacific which could legitimately claim a mandate to host a RTAC, the PIDC Secretariat would be a logical choice in that:

- It has its own legal status flowing from the PIDC Headquarters Agreement with the Government of Samoa, and can sign agreements such as those which may be required to levy charges to fund the RTAC, hold and disburse funds, and has certain privileges and immunities which will benefit the security of operations of any RTAC
- Its members are Immigration agencies, which generally "own" both the national BMS and national Immigration legislation governing the arrival to and departure of people from each member State, meaning they are the natural home of any national Passenger Data Single Window and can perform national BMS checks against API data
- A RTAC is consistent with the existing PIDC Constitution and Members MoU, and the subsequent MoA "*Concerning cooperation and capacity building and the disclosure of information for immigration, border protection, law enforcement and public safety purposes*"
- PIDC is ultimately subject to its membership and governing Board, thus the operations of the RTAC and management and disbursement of its funds remain within the control of the membership.

Other key stakeholders regionally include the PTCCC, which is also based in Apia, Samoa, and OCO. Both will be important in the operation of any RTAC, in terms of coordination of their member agencies and seeking a mandate from them to support and share intelligence and profiles with any RTAC. Both may also be pivotal in assisting with staffing the RTAC, which should include not just Immigration, but also Police and Customs officers from member States as is the case in the CARICOM example.

Additional mandates are also likely required, or at least desirable, from the PIF and PICP, as these will need to give any RTAC the fullest possible regional political support, consistent with the Boe Declaration and Action Plan.

Recommendation 15: CBS strongly recommends that consideration be given to the establishment of a Pacific Regional API Assessment Centre in keeping with the Boe Declaration and Action Plan.

4.4   Costs and Cost Recovery models

A detailed analysis of the financial legislation of PIDC member countries is beyond the scope of this paper, however there will undoubtedly be differences in the legislative requirements of member countries. For example, across member countries a number of different legal and financial systems and influences are in play including British, US and French. Each of these has its

own distinct requirements and processes, which is likely to take some time for countries to work through in order to reach an agreed common approach to mandating and funding a regional approach to API. The development of a common funding model will therefore require a strong commitment from participating governments, negotiation and, ultimately, compromise.

Against this background, options for funding ongoing API arrangements in the Pacific could include:

1. national budget support from participating member States, split between each State based upon traveller volumes; or
2. ongoing donor support; or
3. cost recovery via a levy on passenger tickets or similar; or
4. a combination of some, or all of these.

Of the four options presented above, reliance on consistent budget funding support from internal revenues (Option 1) of member states, many of which are heavily reliant on foreign aid to balance their national budgets and have differing fiscal priorities, is likely to prove the most difficult option to sustain in the longer term.

In the current economic climate, it will undoubtedly be tempting for PIDC members to seek money from wherever they can find it. As mentioned previously, this could lead to donor pressures which may skew the directions set for the development of regional priorities, such as a regional API information-sharing arrangement. CBS hold the view that during tough economic times it is more important than ever for governments to examine their funding strategies closely and be disciplined about the way that they raise money.

Ongoing donor support (Option 2) beyond initial development and establishment of API arrangements in the Pacific region may be slightly less problematic if a compelling case can be made that the ongoing support and operation of the system provides clear benefits to donor countries in effectively pushing their border decision-making out further to the mutual benefit of all parties. The other factor at play is the apparent renewed desire on the part of some donor countries such as Australia and the USA to re-engage with the Pacific, particularly in response to the spread of terrorism, disease and transnational crime. Timely decisions and the formulation of a common approach to donors, perhaps also via the PIF, would be critical to realising the benefits of this option.

Cost recovery via a levy on air and cruise ship passenger tickets (Option 3) in the region may be the most complicated option to establish initially but is likely to prove the most viable option for the provision of necessary ongoing funding. This is because it would likely require legislative arrangements within participating States.

This approach could conceivably fund the individual approach to API implementation, at least for several PIDC members with larger traveller volumes, however it does not address the overall implied higher human and financial costs, nor does it simplify the cost recovery process.

A possibly simpler way of funding such an operation may be outsourcing this, and the associated administration and audit requirements, to a trusted regional partner, external and distinct from individual countries, but still answerable and accountable to them. Were a Regional Organisation such as the PIDC Secretariat itself (or some other organisation perhaps operating under its auspices) to "host" the solution or at least provide a central point of governance for it, clarity that its legal entity status would permit this would be important.

Given the above, if a decision is taken to pursue a regional API solution, the most efficient approach might be to pursue Option 4. above, whereby a donor country (or countries) funds its establishment and first year of operations, or a few years should COVID-19 remain a dampener on regional travel.

In parallel, CBS suggests that a passenger levy should be introduced which would fund ongoing operation of the regional data sharing and assessment centre with any surplus funds committed to funding ongoing development and upgrades of systems and processes. An arrangement of this kind would be highly dependent upon the establishment of an independently established 'Fund' to collect revenue and disburse monies. The operation of such a Fund would require an agreement signed by all participating parties which should clearly circumscribe the activities of the Fund, with robust prudential controls and reporting requirements put in place and, most importantly, **enforced**.

Based upon pre-COVID-19 South Pacific Tourism Forecasts[32] and using the calculations below, it would appear that a charge of USD$1 per arrival and departure from each participating country via ticketing systems would likely provide more than sufficient revenue to cover the annual running costs, and leave funds over to support ongoing development and related initiatives. Concept modelling in US$, based upon the figures detailed in Chapter 3:

- US$ $0.19 (approx.) charge per ticket = ongoing minimal functionality fully sustained.
- USD $1 charge per ticket = full sustainment plus up to a possible USD$5.73 million per annum to expand assessment capability and staffing, with the residual disbursed based upon traveller numbers to each participating state to offset member border management costs, fund national BMS upgrades or installations to accommodate API locally, etc.[33]

It is important to note that these costs do not include the cost of the SITA regional offering at **Annex 5**, which is discussed in section 4.2 above, and are based upon the premise that the RTAC could operate using the basic standard Type-B data feeds from both SITA and ARINC, which is what CARICOM does.

It is open to PIDC and members to consider opting for a CARICOM-style RTAC solution as well as a value-added service such as the SITA Regional offering, however this would require the addition of at least **US$1** to each arrival and departure to ensure feasibility as well as providing a surplus for use of members. This would see the charge rise to US$2 per arrival and departure, which may still be feasible and acceptable. The advantage in pursuing both is that participating members could opt for both the centralised assessment centre provided by the RTAC, as well as a direct feed from SITA (for example) with the value-added service contained in their offering.

As noted in the CARICOM example described at section 4.1 of this report, the development of an agreed funding model that incorporates a traveller levy has not yet gained widespread

---

Recommendation 16: CBS recommends that, unlike CARICOM IMPACS, a model to provide ongoing funding for a Pacific Regional API Assessment Centre, independent of Government budget allocations or donors, be sought from the outset.

---

acceptance among CARICOM member countries and consequently, current operations are supported on the basis of US aid and from within the budgets of participating member countries. Neither the CARICOM JRCC Secretariat nor the authors regard this as an optimal funding model.

---

[32] https://corporate.southpacificislands.travel/spto-releases-2019-2024-pacific-tourism-forecast/
[33] This is an estimate only, and whilst a surplus can be expected, this will vary on costs, and traveller numbers in any given year

Air ticket levies could be collected with little effort via the IATA Clearinghouse, membership of which could be sought by the governing Regional API body.[34] A similar charge would need to be levied more directly upon cruise ship operators for passing on to travellers in their ticketing, and incorporated into fees and charges levied upon individual private aircraft and small craft such as yachts.

Development costs are unknown at this stage, but it is expected development to a full, finished "product" servicing a RTAC could cost US$200,000-$500,000, take anywhere between 1-3 years to establish, and would likely require at least initial donor support, particularly as COVID-19 has severely impacted traveller numbers and hence the national budgets of PICTs. On the more positive side, significant expertise at little or no cost may be drawn upon from ICAO, WCO and UNOCT in establishing key elements of the system, particularly around integration of API data feeds with the assessment tools GTAS and goTravel.

Office set-up and furnishing will be required should a physically co-located centre be chosen. It would be prudent to allow US$150,000 for this, and should a locally-hosted server-based solution be considered over a cloud-based solution, a further $250,000 for key server and communications hardware procurement.

An estimate of ongoing costs involving local or cloud-hosting, support and maintenance, licensing, business-grade internet connectivity, and including basic type-B SITA and ARINC connections of at least US$20k per annum, would see an annual fixed systems costs estimate of US$350,000. Licensing costs should be minimised in any system design, with open-source software and coding utilised wherever possible, along with the cost-free assessment tools mentioned above, and as such, it is likely this cost estimate is at the higher-end.

Assuming salaries and allowances for up to 13 staff including:

- an Executive Director at US$90,000;
- an IT Support and Programming Expert at US$80,000;
- an accounts and office manager at US$25,000 per annum; and
- 10 assessment officers, operating two x 12-hour shifts, with one team off-shift and allowing for leave, averaging salaries of US$25,000 each per annum.

Staffing costs, estimated generously here at the higher end of the likely range, could be expected to reach at US$445,000 per annum, with allowances for seconded officers (posting allowances) and overtime likely to add up to a further US$150,000 per annum, bringing an annual salary estimate to US$595,000.

It is possible that office rental costs will not be required where the RTAC is hosted within the mandate of one of the existing regional organisations, such as PIDC, where rent-free accommodation is an existing benefit of their status and location, however this is not assumed and a figure of US$150,000 has been added for this purpose, as has a further US$50,000 to provide housing for seconded officers from member States. These figures, based upon a location in Apia, Samoa, and also estimated at the higher end of the likely range.

Utilities, personal communications, along with travel and incidentals will need to be accommodated into a main office operating budget of US$100,000 per annum.

---

[34] See https://www.iata.org/en/services/finance/clearinghouse/

Summary table of estimated costs in US$:

Description	Set-up cost	Ongoing (Annual) cost
Office Rental		$150,000
Staff housing (seconded officers)		$50,000
Office fit-out	$150,000	
Hardware procurement (local server solution)	$250,000	$25,000 (annual hardware refresh budget)
RTAC system development, deployment, integration	$250,000 (estimate)	
RTAC System Operation – annual operating and licensing costs		$350,000
Office annual operating budget		$100,000
Salaries, overtime, allowances		$595,000
Totals	$650,000	$1,270,000

To put this into perspective, were all 18 PIDC members, except Australia and New Zealand, to participate, the cost would amount to US$70,500 per member PICT to operate per annum, with costs borne by travellers, not Governments or, ultimately, donors.

> **Recommendation 17:** PIDC members should note the possible funding options for the development and introduction of a regional API arrangement, particularly the option of using donor funding to establish a regional data assessment and information sharing centre with ongoing operational and development costs funded through the imposition of a levy/ticket (Option 4).

4.3 Governance Requirements

The establishment of an API reception and assessment facility, whether regional or individual in implementation, will require:

- Legislative authority for the receipt, custody and sharing of information from within each participating country's Immigration legislation
- Written agreements, such as with carriers, and in the case of a regional implementation, with that organisation.

Model legislation has been suggested at **Annex 2**, which would permit either the individual or regional approaches to API, and also PNR once a decision is made to expand the dataset and analysis. This is suggested where current legislation does not accommodate API, or more broadly accommodate all necessary aspects of information sharing.

4.4 An Implementation Pathway

The following is a suggested pathway to implementation of a Regional Traveller Assessment Centre. As timelines are not certain until the full software design is complete and the necessary

amendments have been made to the legislation of participating PIDC members, this has not been provided, however it should be anticipated that step 15 below is achievable within 3 years of endorsement by the PIDC Board (step 6).

1.	Circulate the final version of this report, gauge support of members, tabulate responses, coordinate clarification and responses as required
2.	Interested members seek support of their governments, including obtaining a firm commitment to urgently initiate legislation and/or policy changes as necessary, and an indication as to whether an individual or regional solution hosted with PIDC (or other body) is the preferred option.
3.	PIDC Secretariat to approach relevant regional organisations, for example, PIF, PTCCC, OCO etc to outline the nature and level of interest from member countries in the adoption of API and whether the individual or regional approach is preferred, outline the prospect that they could provide intelligence and profile inputs, and members could benefit from API data feeds via the RTAC and/or domestic PSDWs, and seek the views and suggestions.
4.	PIDC Secretariat to approach key donors to gauge interest and likely support for each option (Individual or Regional approach)
5.	PIDC Secretariat to prepare a consolidated proposal for the endorsement of the PIDC Management Board.
6.	Following endorsement, should the regional approach be preferred by sufficient members, PIDC Secretariat to: • Confirm availability of start-up funds and support expertise (donor, ICAO, WCO, UNCTO etc) • prepare a detailed implementation plan, • confirm budget, accommodation, staffing & cost recovery arrangements • draft underpinning MOUs and/or information sharing agreements with members and regional partners (PTCCC, OCO etc) and, • depending upon the option chosen, prepare necessary Tender Documentation
7.	PIDC Secretariat to sign MoUs with interested members, commence engagement of donor expertise, and engagement of selected software development provider/s.
8.	Interested members commence necessary legislative and policy change, reallocation and training of staffing and development of internal SOPs in preparation for API
9.	PIDC Secretariat to locate and secure office space, commence recruitment of key RTAC personnel, including Executive Director, Office Manager, IT Expert, and at least several assessment team members.
10.	PIDC Secretariat and RTAC to negotiate and agree API data transmission arrangements with carriers, cost recovery arrangements with IATA Clearinghouse and Cruise Ship Operators
11.	With donor support and/or with software development partner /Business Analyst contracted by RTAC, document the high-level business requirements, as well as: • functional scope • security architecture • solution architecture • integration architecture • infrastructure architecture, • non-functional specifications
12.	Commence system design & build, testing, initial user acceptance testing. Beta and initial production releases as per agreed system rollout plan
13.	Finalise recruitment and training of RTAC Assessment teams, completion of RTAC SOPs

14.	First live testing with API data, depending upon readiness of legislation in recipient countries.
15.	Full live operations commence

5. Conclusions

API is not just a mandatory requirement of all States and Territories, its proper implementation promises to serve national and regional security objectives, whilst providing a better experience for travellers as most will as a result have been vetted and identified for appropriate on-arrival treatment according to assessed risk prior to arrival. It can be applied equally to air and maritime arrivals and departures.

API is fundamentally not a complex tool. It consists of electronically collected, structured and transmitted traveller biodata and flight/voyage data which is available at the time of check-in and wheels-up, or in the case of vessels, actual departure. At its simplest, this can take the form of a spreadsheet.

Despite this, making best use of API is not as straightforward as it seems. PICTs have been slow to implement API for understandable reasons. There are internationally acceptable, cost-free API assessment tools available, however most PICTs lack the human, financial and technical expertise and resources to fully implement the staffing, legislative, governance and systems requirements to enable these. Most lack a BMS which is compatible with API, and although it has been discovered this is not a complete impediment, this is highly desirable to make best use of API data.

Whilst a proper implementation of API promises to enable the diversion of resources away from other less efficient manual processes, such as some forms of Visa on Arrival, it would still require a 24/7 assessment team in many PICTs to derive maximum value from the data. This is a significant constraint for many.

Individual PICTs are open to progress API implementation on an individual basis; however, they would bear the financial, organisational and human resources impacts of this individually as well.

This report has explored two models of how API may be implemented on a regional basis. Perhaps the most promising is that of the CARICOM IMPACS JRCC eAPIS. In this example, a regional forum, CARICOM has, with a mandate provided by member States and enabled in member State domestic legislation, established a regional API assessment centre serving the interests and border security of participant members.

Whilst it may be possible to establish much of the systems architecture of such a facility using the expertise of major airline communications providers such as SITA, the most promising approach appears to be to follow that of CARICOM as this also promises both the greatest member State control, and greatest likelihood of becoming self-funding via a US$1 levy on air and cruise ship arrivals and departures via tickets, or $2 per movement if both this model and a value-added model such as that at **Annex 5** are both pursued.

This funding model is likely to generate sufficient funds to fully operate, staff and maintain a Regional Traveller Assessment Centre, with sufficient funds also to self-fund the installation and/or upgrade of BMS capability within participating members domestic agencies, further value-adding the regional assessment centre.

It is proposed that, should members decide to proceed with a regional API assessment capability, this be attached to an existing Pacific regional organisation such as PIDC, for reasons of convenience, and as these are known bodies, accountable to members. Outsourcing to such a

regional assessment centre would not diminish sovereignty. API data would only ever be available to carriers, the assessment centre, and the receiving member. Most importantly, the decision as to how to treat each passenger as a result of assessments would remain with the individual member PICT, not with the regional assessment centre.

PNR data is a further form of passenger data which should also be integrated into any individual or regional assessment function; however, it is not recommended that this be included in any initial implementation given the complexity of privacy and data retention arrangements which are associated with PNR and the EU.

Interactive API (iAPI) is also not recommended for any initial implementation, given the much greater complexity, particularly in respect of systems integration.

PICTS should approach API implementation cautiously and with deliberate steps, building confidence and capability at each stage. The regional solution proposed by this paper would, through sharing resources and collective intent, most likely realise API implementation sooner in more PICTS than otherwise would be the case. Depending upon the number of participants and eventual cost-recovery model, it is also possible that both the IT systems and human assessment capability could be implemented with no ongoing costs to participating members.

6. Summary of Recommendations

Recommendation 1: Batch API is recommended for any initial implementation in the Pacific.

Recommendation 2: Consideration should only be given to the implementation of iAPI once the human, systems, and legislative capability within agencies and Governments has adapted and expanded to effectively accommodate Batch API.

Recommendation 3: The adoption of PNR should only be considered once the human, systems and legislative capability within agencies has adapted and expanded following API implementation.

Recommendation 4: PIDC members should note that, while ETA or pre-clearance measures, PNR and Interpol SLTD interoperability are not mandatory, they are recommended by ICAO and/or the UNSC.

Recommendation 5: Consistent with the principles of CBM and UNSCRs, consideration should be given to improving PIDC members' border management through:

- the direct acquisition of API systems capability by PIDC members; or
- the central negotiation and procurement of API systems capability by an organisation, such as PIDC, on behalf of all interested members.

Recommendation 6: Members should consider adoption of the standard set of API data fields used for transmission from carriers to border control agencies, as defined by ICAO, WCO and IATA, as prescribed in the *Draft Regulations* at **Annex 2, Schedule 1** of this report.

Recommendation 7: It is highly recommended that some form of API integration be adopted by those PIDC members which have a BMS.

Recommendation 8: Border control agencies that receive data should ensure relevant systems and hardware are up-to-date, and secured behind appropriate physical and software safeguards and controls.

Recommendation 9: It is highly recommended that renewed emphasis be placed on the review and modernisation of PIDC members' Immigration legislation order to create an environment conducive to the introduction of API and information sharing more broadly, consistent with the principles of CBM.

Recommendation 10: CBS suggests that the CARICOM JRCC may be a viable model upon which to base a collaborative Pacific regional API collaborative arrangement.

Recommendation 11: PIDC should consider the implications of SITA's model which highlight the potential for cost-effective "regional" service offerings to Governments facing significant resourcing and capability constraints.

Recommendation 12: It is recommended that, while it is open to PIDC members to implement API connectivity and assessment on an individual basis, the potential benefit of economies of scale will not be realised meaning that the complexity and costs are likely to be greater because at least some checking and assessment of API within each PIDC member country will be required.

Recommendation 13: Consideration should be given to a regional approach to API which would allow smaller PIDC member states which either do not have a BMS, or do not have a BMS which is API capable, to still derive benefit from API data.

Recommendation 14: PIDC members should note that adoption of a regional approach to API would not diminish or absolve PIDC members from their ability and responsibility to also carry out their own assessments against national BMS and other databases, or impinge upon the ultimate sovereignty of members and their data.

Recommendation 15: CBS strongly recommends that consideration be given to the establishment of a Regional Traveller Assessment Centre in keeping with the Boe Declaration and Action Plan.

Recommendation 16: CBS recommends that, unlike CARICOM IMPACS, a model to provide ongoing funding for a Regional Traveller Assessment Centre, independent of Government budget allocations or donors, be sought from the outset.

Recommendation 17: PIDC members should note the possible funding options for the development and introduction of a regional API arrangement, particularly the option of using donor funding to establish a regional data assessment and information sharing centre with ongoing operational and development costs funded through the imposition of a modest levy per ticket (Option 4).

Recommendation 18: PIDC members should review the draft definitions and additional provisions proposed for inclusion in their Immigration Act as outlined in **Annex 2** and adopt as necessary.

Recommendation 19: PIDC members should consider the inclusion of some or all of the definitions and draft provisions to support the introduction of API proposed for inclusion in their Immigration Regulations, as outlined in **Annex 2**.

Annex 1 – Environmental Scan

Status of PIDC members' legislation for introduction of API

Country	Current Legislation	Reviewed	API/PNR Definitions, Information Sharing Provisions	Amendment Required
AMERICAN SAMOA	Citizenship, Alienage and Immigration [Title 41] 1984	Not known	No	Reporting duties Possible amendment to s.41.0504 Info sharing – new provision required
AUSTRALIA	Migration Act 1958 Migration Regulations 1994 Australian Border Force (ABF) Act 2015	Yes	Yes Migration Act Division 2, Part 12B Migration Regulations Part 3 ABF Act Part 6	No
COOK ISLANDS	Entry, Residence and Departure Act 1971-72	2018 Bill 2020 Draft Regs	Reporting duties proposed s.108 & 109 Info sharing Proposed s.174-176 of 2020 Bill Part IV of draft Regulations	Yes – to define API and PNR or provide power to PIO to do so Yes – to share information within CI government & with international agencies
FEDERATED STATES OF MICRONESIA	Title 50 Immigration 2014 Revised Code	2019 Considering recommendations	No reporting duties No Info sharing (recommended in proposed Part 10)	Yes - API provision required Yes - API provision required
FIJI	Immigration Act 2003	Underway – scope not known	Reporting duties Part 3 – s.6 Info sharing s.36(1) limited	No Yes- New provision required incl for API
FRENCH POLYNESIA	French Legislation	Not known	Not known	Possibly
KIRIBATI	Immigration Ordinance 1969	Not known	No reporting duties No info sharing	Yes Yes
MARSHALL ISLANDS	Immigration Act 2006	2017/18 Draft Bill 2018	Reporting duties proposed s.40	Yes – if specific to API No – info sharing

Country	Current Legislation	Reviewed	API/PNR Definitions, Information Sharing Provisions	Amendment Required
		Draft Regs	Info sharing proposed s.92 Draft Regs 51&52	
NAURU	Immigration Act 2014	2016	Reporting duties s.7 No info sharing	Yes – if specific to API Yes
	Immigration Regulations 2014	2019		
NEW CALEDONIA	French Legislation	Not known	No	Yes – from information available
NEW ZEALAND	Immigration Act 2009		Yes	No
NIUE	Immigration Act 2011	Possibly 2021	Reporting duties s. 31 No info sharing	Yes – very weak Yes
PALAU	Citizenship and Immigration - Title 13	Not known	No reporting duties except unlicenced vessels s.1108 No info sharing	Yes Yes
PAPUA NEW GUINEA	Migration Act 1978	Not known	No	New provision required
SAMOA	Immigration Act 2020	2018 Draft Regs 2020/21 being considered	Reporting duties s.33 Information sharing s.58 Reg 119	Minor amendment to Part 9 of Act Yes – if specific to API
SOLOMON ISLANDS	Immigration Act 2012	2018/19 Considering recommendations	Reporting duties Part 5 of Act Part 9 of Regs Info sharing recommended for new Part X	Yes – if specific to API Yes - if specific to API
TOKELAU	Immigration Rules 1991	Not known	No reporting duties No info sharing	Yes - if specific to API Yes
TONGA	Immigration Act 1970	2018/19 Considering Draft Act & Regs	Reporting duties s.18&19 Recommended for new Part 5 Part II of Regs Info sharing recommended for new Part X	Yes - if specific to API Yes - if specific to API

Country	Current Legislation	Reviewed	API/PNR Definitions, Information Sharing Provisions	Amendment Required
TUVALU	Immigration Act 1969	2018 Bill 2019 Draft Regs	Reporting duties s.48 Info sharing recommended for Part X s.84(1)(b)	Minor amendment required to draft Bill Yes - if specific to API
VANUATU	Immigration Act 1972 – Chapter 66	2006	Reporting duties s.10 No info sharing	New provisions required
WALLIS AND FUTUNA	French Legislation	Not known	No	Yes

Annex 2 – Model API Legislative provisions

Below is a set of suggested provisions for the Immigration Act which would provide a legal basis for: the collection, submission and receipt of advance passenger information, the sharing of information between government agencies, nationally and internationally; with carriers; other recognised international agencies; employers and education providers to help them avoid employing or enrolling people without entitlement; and to provide for other related matters.

Model Immigration Act provisions - information protection and sharing

Draft definitions

Some or all of the following draft definitions may need to be inserted into the Interpretation Part of the Immigration Act to support information sharing provisions necessary for the introduction of API.

"advance passenger information" or "API" means the information or data concerning a crew member, passenger or any other person travelling in a craft which is provided prior to the arrival of in the destination country

"advance passenger information system" or "APIS" means the automated electronic data interchange of API; and the screening of API by a person delegated under the Immigration Act and/or a designated Regional Organisation against any Alert List;

"Alert List" means a list of persons who may require additional scrutiny by a border control agency or agencies within a clearance zone prior to receiving permission to enter or depart [country XXX]

"Interpol" means the International Criminal Police Organization

"Regional Organisation" means an organisation delegated by the Minister responsible for Immigration to perform a prescribed function under the Act;

"Regional Watch List" means a list that is maintained by a Regional Organisation used to track the current activity or movements of terrorists, those involved in serious criminal activity, criminal deportees, persons who have been found guilty of involvement with stolen and lost travel documents, and other persons of interest to the intelligence and law enforcement community, or those of health concern;

"SLTD" means the list of Stolen and Lost Travel Documents maintained by Interpol

Draft Section I.   Confidentiality of information

(1)   Any information collected or shared for the purpose of this Act must be held as confidential by a person who has come into contact with such information.

(2)   Information collected under this Act may be released in accordance with agreements made under [*Draft Sections III – VII*] of this Act for:

(a)   the prevention, detection, investigation, prosecution, or punishment of immigration or other offences; or

(b)   the processing of international passengers; or

(c)   reasons relating to national security, the national interest, or in the public interest of [insert name of country].

(3)   The [insert relevant title eg., Chief Immigration Officer] may prescribe in the Regulations the procedures for the sharing of information under this section.

Draft Section II.   Establishment, maintenance and protection of information

(1)   The [insert relevant title eg., Chief Immigration Officer] must establish a record or database of information collected for the purpose of this Act, in any form determined by the [Minister].

(2)   Except with the authorisation of the [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] a person is prohibited:

(a)   from attempting to access, or accessing a register, information system or database; and

(b)   from attempting to disclose or alter, or disclosing or altering any information held in a register, information system or database.

(3)   A person who breaches this section commits an offence.

Draft Section III.   Information shared domestically

(1)   The [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] may enter into inter-agency information sharing agreements with other prescribed national government agencies on a need-to-know basis in accordance with relevant domestic laws and policies applying to informed consent and privacy.

(2)   The content and conditions applying to the sharing of information under a national inter-agency agreement are prescribed in the Regulations.

Draft Section IV.   Information shared with overseas agencies and carriers:

(1)   In accordance with [*Draft Section I(2)*] of this Act, information may be shared with an overseas government agency or other recognised agency or international carrier:

(a)   by a person authorised by [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] for the purpose of detecting, preventing, investigating, prosecuting and responding to offences or suspected offences in [insert name of country] or the country concerned; or

(b)   by a person authorised by [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] for the purpose of processing international passengers and crew.

(2)   The [insert relevant title] may prescribe in the Regulations the procedures for the sharing of information under this section.

(3)   The sharing of information with overseas agencies or carriers regarding the movement of people required by any other Act shall be in accordance with this section.

(4)   In the case of any inconsistency between any other Act and this Act, this Act shall prevail.

Draft Section V.   Advance Passenger Information

The following draft enabling provision would provide the necessary Head of Power for the operation of API

(1) The Regulations may prescribe:

(a)   the requirement that carriers, operators and masters of craft must provide arrival and departure API data;

(b)   the timing, content and procedures for the provision of information under this section;

offences and penalties for failure to comply with the requirements of subsections (1)(a) and (b); and

(d)   acceptable defences and circumstances under which a carrier, operator and master may claim an exemption from the requirements of this section.

If a decision is taken to create a regional organisation to perform a bureau service to, for example, facilitate the exchange of API data, maintain a Regional Watch List and undertake primary screening of passenger data against such a list, an enabling provision may be required in the Immigration Act similar to the following:

Draft Section VI. Information exchange with regional organization providing API data sharing and assessment service

(1)   The [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] may enter into an information sharing agreement with an organisation established to provide an advance passenger information data exchange and assessment service.

(2)   The [insert relevant title] may prescribe in the Regulations the procedures for the exchange of information under this section.

Model Regulations governing the collection, protection and sharing of information

Draft definitions

It may be necessary to insert some or all of the following definitions into the Interpretation Part of the Regulations to support information sharing provisions necessary for the introduction of API:

"API Data" is the data referred to in Schedule 1

"API hit" means a name present in the Regional Watch List Systems or Alert List

"commercial aircraft" means an aircraft which engage in transporting passengers or goods for monetary gain;

"private aircraft" means any aircraft which is not a commercial or state aircraft;

 "technical stop" or "stop for non-traffic purposes" means an aircraft or vessel arriving for purposes of refuelling, repairs, emergency or a similar purpose other than taking on or discharging passengers, baggage, cargo and/or mail;

"vessel" means any ship, boat, yacht or other floating or submersible transportation by means of which persons can travel across international borders

Draft Regulation 1. Information collected and shared in confidence

(1)   In accordance with [*Draft Section I(2)* of the Act], all information requested and collected under the Act is classified as confidential and must only be:

(a)   collected and accessed on a need-to-know basis, by officers with a specific delegation issued by [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] to collect information under the Act; and

(b)   shared with another party on the basis of a written instruction from the [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] for:
    (i)   the prevention, detection, investigation, prosecution, or punishment of offences or suspected offences against this Act or any other Act; or
    (ii)   the processing of international travellers; or
    (iii)   the security; and
    (iv)   the national interest of [insert name of country].

Draft Regulation 2.   Maintenance and protection of information

(1)   Border control information obtained from travellers or from other governments, carriers and national and international agencies or a Regional Organisation must be consolidated and held in a Border Management System and/or some other central database in accordance with [refer to relevant section of the Act].

(2)   Information collected and held in accordance with clause (1) of this regulation must be made available to other [insert name of country] government agencies on a 'need to know' basis under a national inter-agency agreement signed by [insert relevant title eg., the Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., the Chief Immigration Officer] and the relevant agency Head in accordance with [*Draft Regulation 3*].

(3)   The [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] must ensure that appropriate procedures and controls are in place to maintain, protect and report on information received or released in accordance with national privacy and information protection standards and legislation including, but not restricted to:
    (a)   clear and current instructions regarding the accurate and timely keeping of records of information released/received;
    (b)   the maintenance of effective data access controls and adherence to prescribed data security standards;
    (c)   the maintenance of current and appropriate delegations issued under the Act; and
    (d)   a comprehensive monitoring and audit program to ensure the integrity of access controls and information transfers.

Draft Regulation 3.   Information shared under national inter-agency agreement

(1)   Except for the provisions of [*Draft Regulation 1*], the [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] shall only authorize the sharing of information with a prescribed national government agency:
(a)   under a national inter-agency agreement; and
(b)   in accordance with relevant domestic laws and policies applying to informed consent and privacy.

(2)   A national inter-agency agreement shall specify the:
(a)   Head of Power used to authorise the sharing of information;
(b)   intended recipient of the information;
(c)   purpose for which the information is released;
(d)   originating agency controls around the storage of the information and/or further release of the information;
(e)   specific content of the information; and
(e)   form and frequency of release.

Draft Regulation 4.   Information shared with overseas agencies and carriers

(1)   Information may be shared with an overseas government agency, other recognised international agency, or carrier :
(a)   under an international bi-lateral or multi-lateral agreement signed by the [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] for the purpose of detecting, preventing, investigating, prosecuting and responding to offences or suspected offences in [insert name of country] or the country concerned; or
(b)   where authorised by the [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] for the purpose of
(i)   processing international travellers; or
(ii)   the border security and national interest of [insert name of country].

(2)   The release of information to any overseas government or recognised international agency, other than for the purposes of sub-clause (1)(b)(i), shall only be in accordance with a written authority of the [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer] which shall specify the:
(a)   Head of Power used to authorise the sharing of information;
(b)   intended recipient of the information;
(c)   purpose for which the information is released;
(d)   originating agency controls around the storage of the information and/or further release of the information;
(e)   specific content of the information; and
(f)   form of the information and frequency of release.

(3)   Disclosure of information regarding the movement of travellers to overseas government agencies, other recognised international agencies or carriers required by any other Act shall be in accordance with [insert reference to

section(s)] of this Act and these Regulations, and in the case of any inconsistency between any other Act and this Act, the Immigration Act shall prevail.

Draft Regulation 5   Use and retention of Advance Passenger Information

(1)   API shall only be used for the purposes of the Act and Regulations.

(2)   API collected under this his Act for entry screening purposes shall be retained for a period not exceeding 3 years from the date of travel.

(3)   Nothing contained in clause (2) shall apply to data copied from the APIS into any other data base system to which a different data retention schedule applies.

Draft Regulation 6   Duty to provide Advance Passenger Information

(1)   This Regulation applies to a craft which:

         (a)   is expected to arrive in [country]; or

         (b)   is expected to leave [country].

(2)   In accordance with clause (1), the operator, captain or master of every craft shall provide to the [*insert title eg., Chief Immigration Officer*] and/or any prescribed Regional Organisation, the API and data relating to the flight or voyage as set out in Schedule I to these Regulations.

(3)   The API provided pursuant to this section must be provided within the timeframes set out in Schedule 2.

(4)   The [*insert title eg., Chief Immigration Officer*] may by instrument in writing vary or replace any or all of the requirements set out in Schedules 1 and 2.

(5)   The Minister may, in consultation with the *[insert title eg., Chief Immigration Officer*], waive the requirements of clause (2) in such circumstances and subject to such conditions as the Minister may prescribe where the craft is –

         (a)   a military or law enforcement craft; or

         (b)   on official state business.

Draft Regulation 7   Craft arriving for non-traffic purposes or making a technical stop

(1)   Nothing in (*Draft Regulation 6*) applies to a craft which makes a technical stop or lands, berths, anchors, or otherwise arrives for non-traffic purposes if the arrival is –

(a)   required by any statutory or other requirement relating to navigation;

(b)   compelled by any emergency, accident, unfavourable weather conditions, or other necessity; or

(c)   authorised by the [*insert title eg., Chief Immigration Officer*].

(2)   Where a craft arrives or stops for any of the reasons outlined in subclause 1 the operator, captain or master shall –

(a)   report to the competent authority or an officer;

(b)   not without the consent of an officer, permit any of the crew or passengers to disembark from the aircraft or vessel; and

(c)   comply with any directions given by an officer in respect of any crew, or passengers carried on the aircraft or vessel.

(3)   A passenger or member of the crew of the craft shall only disembark from the craft with the approval of the [*insert title eg., Chief Immigration Officer*], and all such persons shall comply with any directions given by the [*insert title eg., Chief Immigration Officer*].

(4)   An operator, captain or master who fails to comply with or acts in contravention of this regulation commits an offence.

(5)   Notwithstanding subclause (4), the disembarkation of passengers or crew members from the craft shall not constitute an offence, where the disembarkation is necessary for reasons of health, safety or the preservation of life.

Draft Regulation 8   Sharing of API with regional data exchange and assessment organisation

This following Draft Regulation could be considered in situations where a PICT elects to participate in a regional arrangement for the provision of API data exchange and assessment services by a designated Regional Organisation.

Note: Such an arrangement should be advisory only and ultimate responsibility for decisions as to whether a person is to be admitted or refused entry to the member country still rests with decision makers delegated under the country's Immigration Act.

(1)   The [insert relevant title eg., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer]:
(a)   may enter into an agreement with a Regional Organisation to:

(i)   provide a regional bureau service for the reception, exchange and assessment of API data via an APIS;

(ii)   conduct screening against Regional Watch Lists and Interpol indices including the SLTD database of crew members and

passengers on craft that enter into, depart from [country] on behalf of [enter name of country]; and

(iii) communicate details of any assessment of passengers and crew to an officer designated by the [insert title of alternative authorising officer as necessary eg., Chief Immigration Officer].

(b) shall:

(i) if requested, allow a person who is a passenger or member of the crew from a craft to access his personal details maintained in the APIS to ensure its correctness;

(ii) for the avoidance of doubt the person is not entitled to have access to any alert or related information contained within a Regional Watch List or Interpol database;

(iii) determine, after consultation with such Regional Organisation, the admissibility to [insert name of country] or otherwise of a person; and

(iv) assess the sufficiency, and error rates in review of API transmissions for each journey.

Draft Regulation 9   Duties of carriers following communication of API assessment

(1) An officer may communicate to a carrier, captain or master of a craft the results of assessment of API data in the manner prescribed by the [insert relevant title e.g., Minister responsible for Immigration] or [insert title of alternative authorising officer as necessary e.g., Chief Immigration Officer].

(2) That communication may contain a directive that

(a) where the craft has not departed the port of origin, that;

(i) a person is not permitted to board the craft if they have not yet boarded, or

(ii) a person must be disembarked if they have boarded, or

(b) where the craft has departed the port or origin, that a person be restricted on board and not permitted to disembark the craft on arrival unless otherwise directed by an officer.

(3) Carriers, captains and masters of craft are obliged to comply with the directions in clause (2) except where it can be shown to the satisfaction of the [insert relevant title e.g., Chief Immigration Officer] that, in the case of clause (2)(a)(ii), doing so would unduly delay scheduled departure times of the craft.

Draft Regulation 10   Offences

(1) A carrier, captain or master of a craft who:

    (a)   fails to comply with (draft Regulations 6, 7 or 9), or

    (b)   who intentionally or recklessly provides erroneous, faulty, misleading, incomplete or false API or transmits the API in an incorrect format;

shall be guilty of an offence which:

    (c)   upon conviction in a Court may be fined to a maximum of $XXXX; or

    (d)   upon payment within 28 days of service of an infringement notice issued by the [insert relevant title eg., Chief Immigration Officer**]** requesting payment of [50% of the maximum financial penalty], shall be regarded as conclusively resolved without prosecution or conviction.

(2)   Defences to subclause (1) shall include:

    (a)   in the case of subparagraph 1(a), circumstances where the operator, captain or master of a craft has had to enter the country in emergency circumstances or due to stress of weather; and

    (b)   where the API provided is inaccurate and the operator, captain or master of the craft satisfies the **[**insert relevant title eg., Chief Immigration Officer**]** that the error was not made knowingly or recklessly then notwithstanding any other provision of this Act, the operator, captain or master may not be charged with an offence.

Draft Schedule 1
(Pursuant to *Draft Regulation 2(2)*)

1. ADVANCE PASSENGER INFORMATION - AIRCRAFT

Data shall be transmitted in the current UN/EDIFACT PAXLST format published by WCO, IATA and ICAO. It may also be transmitted in another format, where agreed or directed by a designated Regional Organisation or the [Minister/Secretary/PIO/CMO as appropriate].

(a)   Flight Information (Header Data)

- Airline Code and Flight Number
- Last Place/Port of Call for Aircraft
- Place/Port of Initial Arrival for Aircraft
- Scheduled Local Departure Dates/Times
- Scheduled Local Arrival Dates/Time
- Subsequent Place(s)/Port(s) of Call within the Country (for Progressive Flights)
- Place/Port of Final Destination within the Country (for Progressive Flights)
- Number of Passengers and Number of Crew Members

(b)   Data relating to each individual passenger or crew member:

- Official Travel Document Number
- Issuing State or Organization of the Official Travel Document
- Official Travel Document Type
- Expiration Date of Official Travel Document
- Surname/Given Name(s)
- Nationality
- Date of Birth
- Gender

(c)   Additional Data elements as available in the airline system

- Seat Assignment
- Bag Tag Identification
- Checked Bag Quantity
- Traveller's Status
- Place/Port of Original Embarkation
- Place/Port of Clearance
- Place/Port of Onward Foreign Destination
- Passenger Name Record Locator Number (or unique identifier)

(d)   Additional data

- Visa Number
- Issue Date of the Visa
- Place of Issuance of the Visa
- Other Document Number Used for Travel

(e)   **Data relating to the Reporting Party**

- Reporting Party Name
- Reporting Party Telephone Number
- Reporting Party Facsimile Number
- Reporting Party Email Address

2.   **ADVANCE PASSENGER INFORMATION – MARITIME CRAFT**

Data shall be transmitted in the current UN/EDIFACT PAXLST format published by WCO, IATA and ICAO. It may also be transmitted in another format, where agreed or directed by a designated Regional Organisation or the [*Minister/Secretary/PIO/CMO as appropriate*].

(a)   **Voyage Information (Header Data)**

- Vessel Identification Number
- Vessel Name
- Country of Registration
- Agent/Owner
- Call Sign (if applicable)
- Scheduled Departure Date
- Scheduled Departure Time
- Scheduled Arrival Date
- Scheduled Arrival Time
- Last Place/Port of Call of Vessel
- Place/Port of Vessel Initial Arrival
- Subsequent Place/Port of Call within the country
- Number of Persons on board

(b)   **Data relating to each individual passenger or crew member:**

- Official Travel Document Number
- Issuing State or Organization of the Official Travel Document
- Official Travel Document Type
- Expiration Date of Official Travel Document
- Surname/Given Name(s)
- Nationality
- Date of Birth
- Gender

(c)   **Additional Data elements as available in the shipping reservation or manifest system**

- Cabin, Deck or Seat Assignment
- Bag Tag Identification
- Checked Bag Quantity

- Traveller's Status
- Place/Port of Original Embarkation
- Place/Port of Clearance
- Place/Port of Onward Foreign Destination
- Passenger Name Record Locator Number (or unique booking identifier)

(d)   Additional data

- Visa Number
- Issue Date of the Visa
- Place of Issuance of the Visa
- Other Document Number Used for Travel

(e)   Data relating to the Reporting Party

- Reporting Party Name
- Reporting Party Telephone Number
- Reporting Party Facsimile Number
- Reporting Party Email Address

Draft Schedule 2

(Pursuant to *Draft Regulation 3*)

Timeframe

1.   In the case of arriving commercial aircraft, no later than 40 minutes prior to departure from the last port of embarkation abroad;

2.   In the case of arriving private aircraft, no later than 40 minutes prior to the departure from the last port of embarkation abroad;

3.   In the case of an arriving vessel, no later than 24 hours prior to arrival;

 4.   In the event of any changes to the arriving flight/vessel header data or data relating to an individual on board, an updated API file is required prior to departure of the aircraft from the last port of embarkation abroad or arrival of the vessel.

5.   In the case of departing vessels and aircraft an API file is required five (5) minutes immediately following take-off or departure.

Annex 3 – Stakeholder feedback on collection, storage and sharing of information

The PIDC and IOM/ACP-EU are active in promoting the reform of immigration legislation and operations in the Pacific, particularly the legislative and procedural modernisation program and also via other projects, including strategic planning, training and targeted research. Under their auspices, over the past decade, there has been a considerable number of face-to-face consultations with both government and non-government stakeholders in several PIDC member countries, including Federated States of Micronesia, Tonga, Tuvalu, Samoa, Solomon Islands and the Republic of the Marshall Islands, to solicit feedback and opinions about the operation of current immigration arrangements. The following is a synthesis of the views expressed in these consultations which relate to information sharing which, as can be seen, fall into three main areas. Stakeholders want:

Legislation
- The power to share information to be clearly prescribed in primary legislation (Act).

- Immigration Act should have primacy over all other state or national legislation for people movement in and out of the country.

- Immigration legislation to give greater weight to the issues of national security and control.

- Immigration legislation to more clearly outline carrier responsibilities and penalties to address non-compliance.

- The Immigration Act to be flexible in providing an enabling provision for immigration to share information so that other law enforcement/partner agencies can access limited fields of information that is of interest to specific partner organisations.

- The Immigration Act to provide the authority to stop travel based on a health alert.

- Immigration legislation should be future proofed in regards to technological advancement like API, electronic applications and payments, smart gates and biometrics.

Information Sharing
- Formalised data sharing standards and reporting protocols across government and between governments including inter-agency agreements and MoUs.

- Improved processes to capture data and to reduce duplication of information collected from passenger cards and declarations.

- Border control information from participating agencies to be held in a central database which is accessible by relevant agencies and parties on a 'need to know' basis.

- An increased level of access to the BMS to facilitate the sharing of relevant information with partner agencies.

- A comprehensive national alert list to which all border control agencies contribute and draw from.

- Active management of alert lists and systems to ensure alerts are current and that a clear owning agency or unit is identified for each alert

- Identified anomalies and gaps in entry and exit clearance processes to be addressed and streamlined to balance facilitation and control.

- Improved border management through the acquisition of APP/API systems capability.

- A streamlined online visa application process.

Greater Cooperation

- More cross-agency management level engagement.

- Better education of airlines on their responsibilities in the movement of passengers who do not possess all the documentation for entry into the country and what they need to undertake under the carrier responsibility requirements

- Governments to consider leveraging other States' border management capabilities to improve entry and exit processes and mitigate risk.

- A common approach to negotiating access to third party information.

- A common approach to obtaining foreign government assistance, with regard to improving information flows in border management.

- Upgraded security measures and increased monitoring and reporting of people movements in the light of increasing people flows, new air routes and carriers accessing countries as well as heightened national security.

Annex 4 – References and Further Reading

4.1   International Law

- Convention on International Civil Aviation (the Chicago Convention) – available at https://www.icao.int/publications/pages/doc7300.aspx
    - Annex 9, at https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

4.2   Integrated or Coordinated Border Management

- Coordinated border management: from theory to practice" by Mariya Polner, World Customs Journal, 2011, Vol 5, No. 2, pages 49-64 - http://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/coordinated-border-management.aspx

- World Customs Organisation, Coordinated Border Management Compendium, 2015, available at http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/cbm-compendium.pdf?la=en

- Tom Doyle, "The Future of Border Management", Chapter 2, World Bank – Border Management Modernisation, 2011, available at http://documents.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf

- McLinden, Gerard, "Collaborative border management : a new approach to an old problem", 2012, World Bank, available at http://documents.worldbank.org/curated/en/693361468331207794/Collaborative-border-management-a-new-approach-to-an-old-problem

4.3   Traveller Identification, Passenger Data Exchange

- CARICOM IMPACS website at https://caricomimpacs.org/about-us-v1/

- ICAO TRIP Strategy and related supporting documentation, available at https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx and specifically
    - ICAO TRIP Guide on Border Control Management 2018, available at https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf

- ICAO TRIP Strategy Compendium, 2017, available at https://www.icao.int/Security/FAL/TRIP/Documents/9161_ICAO__icao-trip-Compendium_v15_HIRES_no_Spine.pdf

- ICAO API Guidelines and PNR Reporting Standards - https://www.icao.int/security/fal/sitepages/api%20guidelines%20and%20pnr%20reporting%20standards.aspx

- ICAO Document 9303 – Machine Readable Travel Documents – available at https://www.icao.int/publications/pages/publication.aspx?docnum=9303

- IATA – API-PNR Toolkit - https://www.iata.org/en/publications/api-pnr-toolkit/#tab-1

- WCO – API Guidelines and PNR Reporting Standards, http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

4.4 Compliance and Risk Management

- WCO Customs Risk Management Compendium – available at http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/risk-management-compendium.aspx

- Chapter 6, World Bank – Border Management Modernisation, 2011, available at http://documents.worldbank.org/curated/en/986291468192549495/pdf/588450PUB0Bord101public10BOX353816B.pdf

- The Revised Kyoto Convention – World Customs Organisation – Convention and related resources at http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv.aspx

4.5 Trans-National Crime & Security

- UNODC - Transnational Organized Crime in the Pacific: A Threat Assessment (2016) – available from https://www.unodc.org/documents/southeastasiaandpacific/Publications/2016/2016.09.16_TOCTA_Pacific_web.pdf

- Pacific Islands Forum Secretariat Website – Security, available at https://www.forumsec.org/security/#1509850993375-113a6d90-5fac

- UNODC - Manual on International Cooperation in Criminal Matters related to Terrorism, 2009, available at https://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/English.pdf

4.6 General reading

- *Border Security, Migration Governance and Sovereignty, Susan* Martin and Elizabeth Ferris (IOM 2017) – *available at https://publications.iom.int/books/border-security-migration-governance-and-sovereignty*

- *International Centre for Migration Policy Development (ICMPD) -* https://www.icmpd.org/home/
  - *Policy Brief: Crossing borders in the next 15 years: How should and will border management develop? -* https://www.icmpd.org/fileadmin/user_upload/12_01_18_BM_Policy_Brief.pdf
  - *Other migration-related links -* https://www.icmpd.org/publications/useful-links/

- *International Monetary Fund (IMF) - Regional Economic Outlook: Asia Pacific May 2018 -* *https://www.imf.org/en/Publications/REO/APAC/Issues/2018/04/16/areo0509*

- *International Organisation for Migration (IOM) – www.iom.int*
  - *World Migration Report 2020 -* https://www.un.org/sites/un2.un.org/files/wmr_2020.pdf
  - *Global Migration Indicators 2018 - https://publications.iom.int/books/global-migration-indicators-2018*
  - *Glossary on Migration - https://www.iom.int/key-migration-terms*
  - *Migration Data Portal -* https://migrationdataportal.org/
  - *Migration and the 2030 Agenda: A Guide for Practitioners - https://migrationdataportal.org/tool/migration-and-2030-agenda-guide-practitioners*
  - *IOM Migration Governance Framework (MiGOF), 2015, available at https://publications.iom.int/system/files/migof_brochure_en.pdf*

- *Migration Policy Centre -* http://www.migrationpolicycentre.eu/

- *Migration Policy Institute –* https://www.migrationpolicy.org/
  - *Immigration Data Matters (March 2018) -* https://www.migrationpolicy.org/research/immigration-data-matters

- *Pacific Island Statistics -* https://prism.spc.int/ - soon to be moved to https://sdd.spc.int/

- *PIDC Framework for Immigration Legislation - https://www.pidcsec.org/legislation/*

- *United Nations Department of Economic and Social Affairs – Population Division, Migration Data -* https://www.un.org/en/development/desa/population/migration/data/index.asp

- *UNHCR – www.unhcr.org*
  - *Asylum and Migration https://www.unhcr.org/en-au/asylum-and-migration.html*

- United Nations Sustainable Development Goals - https://www.un.org/sustainabledevelopment/sustainable-development-goals/

- *World Bank Pacific Possible Report (2017)* – https://documents.worldbank.org/curated/en/168951503668157320/Pacific-Possible-long-term-economic-opportunities-and-challenges-for-Pacific-Island-Countries

    - *Tourism sub-report -* https://documents.worldbank.org/curated/en/524541503688261330/Tourism

Annex 5 – SITA proposal for the supply and ongoing operation of an API/PNR gateway

The SITA proposal attached assumes a model involving a 'community offering' on behalf of PIDC members, excluding Australia and New Zealand which already have API/PNR/APP. The costings are based upon scenarios which envisage the participation of 5, 10, and 18 member countries representing an estimated 2.33m, 3.05m and 4.16m travellers respectively. The indicative pricing at Part 6 of the proposal includes an annual fixed charge of $360,000, which applies regardless of the number of members that elect to participate, plus a volume-driven variable fee per transaction, with the transaction unit cost reducing progressively from $0.90 to $0.40 as the number of travellers increases above pre-defined thresholds up to a maximum of 5m passengers.

Please note: This Annex is Commercial in Confidence, and should not be published or released to any parties outside the PIDC membership without the permission of the PIDC Secretariat.

SITA API PNR GATEWAY

Service Overview & Indicative Community Costing

Secure your country with a high quality seamless access to all traveller data

Pacific Immigration Development Community (PIDC)

31 August 2021

SITA

Company Name and Contact Information

Company Details

Company Details: SITA

Division: Border Management

Website: www.sita.aero

Contact Details

Contact: Andrew Philips

Title: Head of Sales - AUSPAC

Telephone: +61 466 328 859

Email: andrew.phillips@sita.aero

Email: bordermanagementbids@sita.aero

Correspondence Address:

Contact: Khaled Elayyan

Title: Director, Global Sales & Solutions Specialist

Telephone: +971 50 5519861

Email: Khaled.elayyan@sita.aero

TABLE OF CONTENTS

1.   Introduction

The collection and processing of advance passenger information (API) and passenger name record (PNR) data is an essential component to helping protect your national borders from terrorism and other threats, including health pandemics without compromising the need of low-risk traveller to travel quickly and effortlessly.

There can be few aspects of a nation's activities that receive the same scrutiny as border control, whether on land, sea, or air. Maintaining a robust and secure border means travellers are often greeted by long delays at border control. This can negatively impact traveller overall experience when visiting your country.

Citizens expect to be able to enjoy legitimate travel, tourism, and trade without the inconvenience of long delays. However, governments have no choice but to work on the side of caution and travellers have come to accept that such delays are sometimes the inevitable price of security.

The need to ensure strong sovereign borders and accommodate a rapid expansion in traveller volumes requires a new paradigm. Governments, in partnership with carriers and infrastructure operators, are transforming border processes using a layered intelligence-driven, risk management approach, leveraging innovative new technology to manage risk as far away from national borders as possible with border systems that are robust, agile, scalable, and seamless for travellers.

The SITA layered framework for border security underpins all capabilities

SITA adopts a holistic framework integrating all solution components together with common identity, case management, and rule engine capabilities under a shared business architecture. In particular:

- Ahead of travel, the agile **SITA Travel Authorization** component collects all required information from applicants through the use of visas and travel authorizations. Verifying documents, checking biographic and biometric identity claims, enforcing data quality and standards, integrating applications with national, international and Interpol watch lists, and maintaining a configurable design that ensures rapid compliance with changing immigration policies and conditions.

- **SITA Health Protect** provides passenger cloud-based declaration for passengers, allowing for the digital collection of important contact and health related information, and verification of major Health Pass certificates. This can be deployed in 26 days.

- From the moment that travel is booked, the **SITA API PNR Gateway** data feeds commence, triggering further alert checks, and enriching information already obtained about a traveller for comparison with the relevant risk profiles Countries with SITA's Advance Passenger Processing (APP) they can export the border with DO NOT BOARD directive issued to airlines, keeping those without the correct visas or travel permits as well as those that pose a risk as far away from national borders as possible.

- **SITA Intelligence and Targeting** solution is configured and tested with simulator capabilities, using existing biographic and biometric data holdings to build alert lists and risk profiles that trigger real-time decisions and interventions at every layer.

- At arrival, the **SITA Entry Exit capability** is already primed with advance information about travellers, and with directives regarding any further interventions or risk treatments required. Following identity verification, travel details are recorded, and cross referenced in the Entry Exit database and also national movements database.

SITA Experience

For SITA, rapid deployment is achieved using a pre-built, out-of-the-box design. By utilizing existing infrastructure and secure data services, the solution is cost effective and robust. Continual investment by SITA in product development ensures the solution will remain effective, both technically and operationally, for years to come.

SITA has unparalleled connectivity with the air travel industry, which has been developed over 70 years. SITA is the global leader in border solutions with a strong record of successful delivery and global 24x7 support infrastructure.

SITA has been helping the air transport industry respond to border control challenges for over 20 years. Alongside our partners in the air transport industry, we have the resources and expertise to provide secure borders and efficient passenger journeys.

GLOBAL PRESENCE

4,700 EMPLOYEES

140 NATIONALITIES

60+ LANGUAGES SPOKEN

SITA SUPPORTS ALMOST EVERY AIRLINE AND AIRPORT IN THE WORLD

2,800 CUSTOMERS — AIRLINES, AIRPORTS, SERVICES AND GOVERNMENTS

200 COUNTRIES & TERRITORIES

1,000 AIRPORTS

NEARLY EVERY PASSENGER TRIP RELIES ON OUR TECHNOLOGY
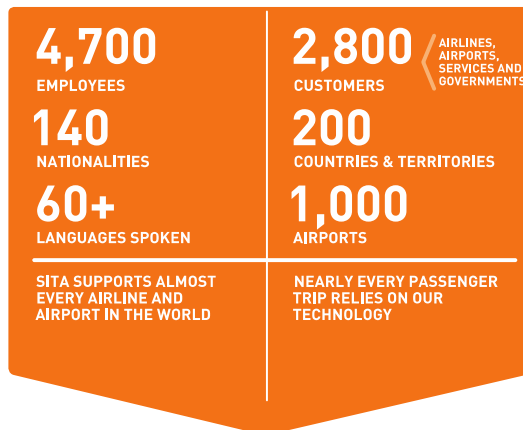
NETWORK AND INFRASTRUCTURE

95% OF ALL INTERNATIONAL DESTINATIONS COVERED BY SITA'S EXTENSIVE NETWORK

13,500 AIR TRANSPORT SITES CONNECTED BY SITA VPN NETWORKS

700 AIRPORTS TO HAVE AIRPORTHUB™ GLOBAL CONNECTIVITY PLATFORM BY 2017
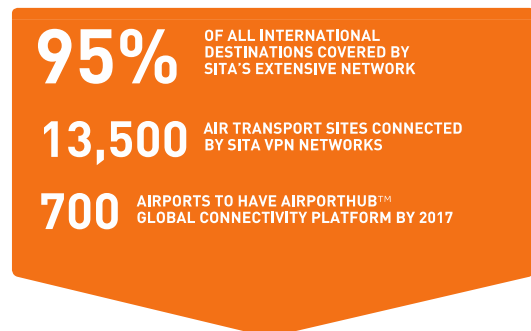
Figure 1. SITA has been helping nations secure their borders for over 20 years. SITA API PNR Gateway connects carrier passenger data with border control systems to help carriers ensure compliance with the countries they fly to and from.

2.   Executive Summary

SITA API PNR Gateway enhances and future-proofs your approach to border management by consolidating traveller information - to, from and through your country. It has been developed using our global border management experience and unparalleled track record in delivery.

By adopting SITA's API PNR Gateway, you will quickly generate improvements in your systems, rapidly freeing up resources for use elsewhere: you will be able to:

- Receive messages in the formats you require

- Ensure the full coverage of travellers (Passengers and Crew)

- Simplify information receipt through a single connection

- Validate all sent information to ensure maintenance of data quality and coverage

- Have the system operational in as little as six weeks

When considering the implementation of a new border control system, you should ask yourself:

- How can we stop the threat before it reaches our borders?

- How can we best use the passenger information available from bookings and manifests?

- How do we collect usable data when passenger's check-in and analyse it before they reach our country?

- Can I merge all the traveller information received from airlines into a single feed?

- How fast can I access this information?

SITA API PNR Gateway for Governments:

Delivering the right data,

at the right time,

from the right Carriers

in the right format.

SITA

3.   Access full traveller details

SITA API PNR Gateway provides seamless access to all passenger information

It combines and integrates PNR, API, and DCS (Departure Control System) data into a single, high-quality data feed. This enables analysis and assessment by your existing border management control systems. You will have secure access to carrier data for viewing, searching, retrieval, statistical analysis, reporting, and administration of the system.

Our continual investment ensures your SITA API PNR Gateway will remain effective, both technically and operationally, for years to come.

3.1   Gateway Data Types

Our SITA API PNR Gateway provides full information on each traveller through the provision of the following data types:

- **Passenger Name Record (PNR)** – Created at the point of booking, the PNR contains complete traveller data and check-in data. Delivered at specified time frames prior to departure (72, 48, 24 and / or 0 hours prior to departure).

- **Advance Passenger Information (API)** – This data is also referred to as a plane's manifest data. It is the confirmation of all travellers who boarded the plane and is only confirmed once the plane has closed its doors.

- **Departure Control System (DCS)** – This data provides you with a snapshot of the data collected at the airport.

3.2   Message formats

PNR, API, and DCS message types can be received using industry standards and transmitted to PIDC in various formats. This means:

- The SITA API PNR Gateway provides PIDC with a data feed that is easy to integrate into your security systems

- Both data providers and data receivers are insulated from system and format changes at either end

International standards issued by IATA / ICAO / WCO are widely established for the submission of API data, with the message type being UN / EDIFACT PAXLST. As new versions of this format are released every year, carriers submit data in varying versions of the format depending upon their system and supported version. Our API PNR Gateway supports receipt of API data in multiple versions of multiple formats.

For PNR, the IATA PADIS (Passenger and Airport Data Interchange Standards) group has defined and published the IATA PNRGOV EDIFACT specification and will also shortly approve a PNRGOV XML specification. The PNRGOV message format accommodates both PNR and DCS data.

The following data types and message formats are supported:

Data Type	Message Formats Supported from Carriers	Message Formats Supported to Governments
API Data	UN PAXLIST 2003 (02B), 2010 (05B) and 2013 (12B) US/UN EDIFACT v1.02, v1.03, v1.04, v1.05	UN EDIFACT PAXLIST 2003 / 2010 & 2013 US / UN EDIFACT v1.02 / v1.03 / v 1.04 & v1.05 GOVDATA XML
PNR Data / DCS Data	PNRGOV EDIFACT v11.1, v12.1, v13.1, v15.1 PNRGOV XML v13.1 and 15.1	PNRGOV EDIFACT v11.1, v12.1, v13.1, v15.1 PNRGOV XML v15.1 GOVDATA XML
DCS Data	PRL PNL/ADL PFS	

3.3   Data Acquisition and Transmission

The table below shows data acquisition methods from airlines supported by SITA API PNR Gateway

Data Type	Source	Acquisition Method
API	Departure Control System	Type-B Via Carrier Portal
PNR	Reservation System (ARS) or Global Distribution System (GDS)	MQ via SITA GovIDNet AS4 via Internet (For Government)
DCS	Departure Control System	MQ via SITA GovIDNet
PFS/ PNL/ADL	Departure Control System	Type B
PRL	Departure Control System	Type B

3.4   API, PNR and DCS Message Correlation

The API PNR Gateway receives different types of data, at different times, for the same passenger for the same journey. It is useful to link this data together, so when it is viewed later, a user can easily see the booking and manifest data for the passenger journey. This provides a rich set of data about that passenger and that journey which can be used for risk assessment and investigative purposes.

This linking process is called "data correlation" and is performed automatically by the API PNR Gateway when two or more record types for the same passenger on the same flight are received. By analysing the information within the messages (such as booking references,

passport information and traveller names) correlations between the data can be drawn. If a match is found, the data can then be linked.

The following information is used to determine if the messages match:

- **Travel Document**: the document details are compared to determine the score.

- **Frequent Travel Number**: FQTV number is compared to determine the score.

- **Ticket**: Passenger Ticket details are checked to determine the score.

- **PNR Locator**: Passenger PNR Locator number is checked to determine the score.

- **Traveller Name**: Passenger Family Name and Given Name are compared to get the score. A single name score is calculated with a 60% weighting to the Family Name score and 40% weighting to the Given Name score.

3.5   Government Gateway Portal

The Government Gateway Portal (GG-Portal) allows authorised users to search and view the messages (API, DCS and PNR) from airlines and the output messages to government (or downstream systems).

The data can be accessed and viewed by authorized users via a web-based user interface.

The data can be searched by:

- Service

- Message

- Message Type

The data can then be filtered by Message Type, Airline, Flight Number, Route and Date Range. The data is stored within the GG-Portal for up to 5 days after the service has departed.

3.6   API PNR Gateway Portal

The API PNR Gateway Portal provides functionality for the manual submission of API data by airlines via the Internet.

The API PNR Gateway Portal is used for submission of crew and passenger data by

- Airlines that do not have the capability to send API data automatically

- Airlines operating at remote airports, where there is a low level of automation

The API PNR Gateway Portal enables airlines to submit API data as a batch file or manually enter data for each passenger. The batch files are uploaded in a pre-approved CSV file via HTTPS.

4. Secure in the knowledge of data quality

Receiving any or all the above data types and message formats ensures you have the data to hand. But you still need to guard against incorrect data or poor-quality data. Data quality is of critical importance given that what you receive will be used to risk assess travellers coming to, from or traveling through your country. To ensure the data allows you to draw comprehensive and meaningful intelligence, it needs to be error-free.

Data quality has several different dimensions. These include completeness, time, format and meaning. By addressing all four you can get the best quality data for your risk assessment.

- **Completeness** – Refers to whether all the required data for all crew and passengers has been provided

- **Time** – Is the data provided with enough time for you to use it for analysis and to identify potential risks posed by travellers?

- **Format** – Focuses on the data being structured correctly. The data is in the correct fields and all mandatory fields are present

- **Meaning*** – Ensuring the correct meaning of the data. Passport numbers are in the correct format for example **Available in 2022*

SITA API/PNR Gateway is built around these four principles. The tools and processes at the heart of the system ensure each message sent by carriers is checked for completeness and accuracy. This provides assurances that the intelligence pulled from it is of the highest quality.

4.1 Data quality reporting

To ensure data quality, SITA API PNR Gateway performs data validation and reporting.

The SITA API PNR Gateway message validation tool uses the messages' received date and time to compare against the confirmed times for messages to be delivered to the government. The validation tool then saves and stores the time of receipt for each message to track each carriers' accuracy in meeting the timing targets.

For reporting, SITA API PNR Gateway provides users with offline reports containing up-to-date statistics for travellers, comprising of the logging of data received from carriers.

Using the reports, **PIDC** is able to track the data quality provided through SITA API PNR Gateway and provide evidence for conversations with carrier providers. The reports provide a safeguard against inaccurate information being passed from carriers to government systems. This allows effective use of information in analysing and identifying travellers to, from and transiting through your country.

SITA

5.   PIDC Requirements

In terms of delivering Gateway service to you, PIDC require the following traveller data:

- PNR (Passenger Name Record)

- API (Advance Passenger Information)

- DCS (Departure Control System)

Message Format and additional requirements for integration with other systems can be discussed and assessed at latter stages when PIDC confirm their requirements.

SITA

6.   Price and commercial

Although all care has been carried out to ensure that pricing provided is accurate based on SITA's understanding of the requirements and assumed scope, pricing provided below is purely an estimate for budgetary purposes. It does not constitute a formal commercial offer and any final pricing will require the approval of SITA's Business Approval Board.

Please find below API/ PNR Gateway indicative pricing and high-level commercial terms to PIDC based on a community offering model for countries welling to participate.

The countries covered in the community offering are: American Samoa, Cook Islands, Micronesia, Fiji, French Polynesia, Kiribati, Marshall Islands, Nauru, New Caledonia, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis & Futuna.

Australia and New Zealand are not covered in this model since they already have well established systems in place.

Recommended at least 5 countries to participate in the community offering.

Contract term is 3 years

Bracket	Min	Max	Fee	Comments
Annual Fee	NA	NA	360,000	Divided between participating countries
Bracket 1	Zero	1,100,000	0.90	Bracket Delta: 1,100,000 pax
Bracket 2	1,100,001	1,800,000	0.80	Bracket Delta: 700,000 pax
Bracket 3	1,800,001	2,700,000	0.60	Bracket Delta: 900,000 pax
Bracket 4	2,700,001	5,000,000	0.40	Bracket Delta: 2,300,000 pax

SITA can provide consultancy if required, prices available on request.

The pricing structure is based on fixed annual community fees divided equally between participating country and incremental per passenger fee based on total passenger traffic volumes for the community.

The total invoice will be divided between participating countries based on their contribution to the passenger traffic.

The fixed fees and the passenger fees are calculated and invoiced on monthly basis.

The payment term is 30 days from the invoice issuance.

6.1 Community Commercial Modelling Examples

Example One: Starting with 5 Countries

Government	Pax	% of Total Pax	Fixed Fee	Variable Fee	Annual Invoice	3 Years Contract Term
Fiji	1,400,000	60%	72,000	1,122,600	1,194,600	**3,583,800**
French Polynesia	450,000	19%	72,000	355,490	427,490	**1,282,470**
Samoa	260,000	11%	72,000	205,810	277,810	**833,430**
Solomon Islands	130,000	6%	72,000	112,260	184,260	**552,780**
Micronesia	95,000	4%	72,000	74,840	146,840	**440,520**
Total	**2,335,000**	**100%**	**360,000**	**1,871,000**	**2,231,000**	**6,693,000**

Example Two: Growing to 10 Countries

Government	Pax	% of Total Pax	Fixed Fee	Variable Fee	Annual Invoice	3 Years Contract Term
Fiji	1,400,000	46%	36,000	1,026,352	1,062,352	3,187,056
French Polynesia	450,000	15%	36,000	334,680	370,680	1,112,040
Samoa	260,000	9%	36,000	200,808	236,808	710,424
Solomon Islands	130,000	4%	36,000	89,248	125,248	375,744
Micronesia	95,000	3%	36,000	66,936	102,936	308,808
American Samoa	33,000	1%	36,000	22,312	58,312	174,936
Cook Islands	225,000	7%	36,000	156,184	192,184	576,552
Kiribati	60,000	2%	36,000	44,624	80,624	241,872
Tonga	150,000	5%	36,000	111,560	147,560	442,680
Vanuatu	250,000	8%	36,000	178,496	214,496	643,488
Total	**3,053,000**	**100%**	**360,000**	**2,231,200**	**2,591,200**	**7,773,600**

Example Three: 18 Countries Onboard

Government	Pax	% of Total Pax	Fixed Fee	Variable Fee	Annual Invoice	3 Years Contract Term
Fiji	1,400,000	33.7%	20,000	901,003.2	921,003.2	2,763,009.6
French Polynesia	450,000	10.8%	20,000	288,748.8	308,748.8	926,246.4
Samoa	260,000	6.3%	20,000	168,436.8	188,436.8	565,310.4
Solomon Islands	130,000	3.1%	20,000	82,881.6	102,881.6	308,644.8
Micronesia	95,000	2.3%	20,000	61,492.8	81,492.8	244,478.4
American Samoa	33,000	0.8%	20,000	21,388.8	41,388.8	124,166.4
Cook Islands	225,000	5.4%	20,000	144,374.4	164,374.4	493,123.2
Kiribati	60,000	1.4%	20,000	37,430.4	57,430.4	172,291.2
Tonga	150,000	3.6%	20,000	96,249.6	116,249.6	348,748.8
Vanuatu	250,000	6%	20,000	160,416	180,416	541,248.0
Marshall Islands	88,000	2.1%	20,000	56,145.6	76,145.6	228,436.8
Nauru	49,000	1.2%	20,000	32,083.2	52,083.2	156,249.6
New Caledonia	360,000	8.7%	20,000	232,603.2	252,603.2	757,809.6
Niue	17,000	0.4%	20,000	10,694.4	30,694.4	92,083.2
Palau	139,000	3.3%	20,000	88,228.8	108,228.8	324,686.4
New Papa Guinea	420,000	10.1%	20,000	270,033.6	290,033.6	870,100.8
Tuvalu	12,000	0.3%	20,000	8,020.8	28,020.8	84,062.4
Wallis & Futuna	21,000	0.5%	20,000	13,368	33,368	100,104.0
Total	**4,159,000**	**100%**	**360,000**	**2,673,600**	**3,033,600**	**9,100,800**

- No available data on Tokelau

- Passenger traffic is based on approximate numbers of 2019 inbound/ outbound

SITA

6.2   Contractual Terms

- The delivery of the products and services described in this proposal will be subject to a contract to be negotiated between the parties.

- The information provided in this proposal is confidential to SITA. It may not be shared outside your organisation without SITA's express written consent.

- All products, services, company names, trademarks, logos, devices, symbols, or other similar items (whether registered or unregistered) that may be contained within or referred to in this proposal are acknowledged as belonging to or licensed to the originator.

- The prices listed in this proposal do not include custom duties, value added taxes, turnover tax, sales tax and any other tax or duty levied by authorities in relation to the products or services. All such taxes (except any income tax payable by SITA) and/or duties will be charged separately as per negotiated contract.

- The terms of the contract will exclude SITA's liability for consequential losses or indirect losses, loss of revenue, profit, and goodwill.

6.3   Validity Statement

- This proposal and any prices herein are valid for a period of forty-five (45) days from the date of this document (see front cover).

- SITA reserves the right to modify the prices or withdraw the proposal after expiry of the validity period.

6.4   Restrictions to trade, embargoes, and regulatory issues

- The provision of the services under this proposal may be disrupted or prevented by various types of regulations enacted in reaction to the prevailing political environment or to regulated business sectors.

- SITA is subject to the embargoes imposed by the United Nations and European Union and may also be subject to trade and export restrictions of other sovereign states.

- Locally, the provision of services may also be delayed or even prevented by local regulations governing custom declarations or governing certain business sectors or industries.

6.5   Security

- SITA takes and implements technical and organizational measures to maintain the confidentiality, integrity, availability and resilience of processing systems and services as well as of the personal data held within such systems. SITA may update or modify these measures from time to time to upgrade the overall security of the contracted services.

- SITA takes measures to guard against unlawful activities which pose a threat to the confidentiality, integrity, and availability of SITA customers' data in respect of its provision of any contracted service in accordance with:

    o   laws, regulations that are applicable to SITA;

    o   industry practices; and

    o   the applicable service levels for the relevant services

- SITA employees undergo security and privacy training to ensure they comply with ethical business conduct and are able to identify security risks and adequately respond to these in the course of their activities.

- SITA manages security incident response activities in order to minimize any adverse impact to SITA and SITA's customers as well as enable root cause and/or forensics analysis.

7.   Our approach to data privacy

For over 70 years, SITA has been responsible for the personal and operational data of billions of travellers around the world.

This means that almost every traveller's data touches a SITA product at some point in its journey. That's why we've ensured that SITA API/PNR Gateway has been developed to include robust and secure security measures, benchmarked against international best practices.

We take care to respect privacy laws around the world and this product is fully compliant with the European Union's General Data Protection Regulation (GDPR). Internal and third-party audits are undertaken, along with external penetration tests as part of our security practices.

SITA API/PNR Gateway processes your traveller data in a way that satisfies GDPR requirements:

- SITA acts purely as the processor of the data, providing the necessary connection between the controllers of carriers (airlines, ferry, or train operators) and governments.

- SITA API/PNR Gateway reports contain no personal data but are a summary of the data collected. In this instance personal data refers to:

Data Categorization	Data types
Passenger data	Passenger Names
	Passport, visa, and travel document information
	Seat information
	SSR and OSI information
	Agent information
	Ticket information
	Addresses
	Remarks (including FOPs)
	Passenger type
	Frequent Flier Information
	Contact numbers and addresses
Operational Data	Record locators
	Agent comments
	Boarding pass details

- The data passing through our system is only used for purposes agreed with you.

- All information is kept only for the time period needed to transfer it from carriers (airlines, ferries, train operators) to governments. Once the data transaction has been completed all data is securely deleted from the system.

- At no point do we share any of the data or forward it on to other parties (except to other governments who require it for their own traveller processing).

- Data is stored in a secured database and transferred via private secured networks.

- SITA API/PNR Gateway has adopted the best practices set out in ISO 19944 to ensure you are aware of what personal information you are receiving, where it is based and how securely it is handled. Along with all risks associated with the data being handled.

We have developed robust security practices and policies, carrying out frequent impact assessments to ensure the data is safe whilst being processed by our systems.

8.   Why SITA API PNR Gateway for Government?

SITA API PNR Gateway is **your strategic solution** to offload all the concerns with traveller data acquisition programme. While your team remain focused on border security and combating terrorism, illegal migration, and human trafficking.

It is a secure *Data As A Service*, capable of providing a validated data feed for passengers **and crew data** to your government at the right time in the right format.

It will help you reduce resource cost and provide your team with all resources and tools to help them assessing travellers coming to or departing from your country.

With its existing global coverage and SITA team expertise, data will start flowing for analysis in few weeks.

9.   Suggested Next Steps

- PIDC to review service overview and indicative community costing
- Meeting with SITA to present and respond to clarifications
- Refinement of service model
- Revised proposal submitted

SITA