



Unisys Australia Pty Limited
ABN 31 105 642 902

Telephone
61 2 9647 7777
Facsimile
61 2 9647 7000

Unisys Campus
Rhodes Corporate Park
1G Homebush Bay Drive
Rhodes NSW 2138
PO Box 288
Concord West NSW 2138

27 June 2008

Department of Infrastructure, Transport,
Regional Development and Local Government
GPO Box 594
Canberra
ACT 2061
aviationstatement@infrastructure.gov.au

Dear Sir/Madam,

Submission to the Development of a National Aviation Policy Statement

Introduction

Unisys welcomes the opportunity to contribute to the development of a National Aviation Policy Statement. In so doing, we hope to assist you in your deliberations and further inform discussion on some of the issues raised.

We would be happy to provide additional clarification on the issues raised in this submission if it would be of assistance.

Background

Unisys is a global information technology services provider that specialises in services consulting and systems integration, outsourcing and infrastructure and enterprise server technology particularly for Government, aviation and financial services industries. We have particular global market strength in transportation and security (from identity credentialing to network security and surveillance) with a long history of working with the transportation and public sector in New Zealand, the United States, Canada, the United Kingdom, Europe as well as countries in Asia - it is a core competency of our firm.

In Australia, five of Australia's top ten companies (defined by *BRW* top 1000) choose to work with Unisys. Unisys has 2,000 employees distributed across offices in Sydney, Canberra, Perth, Melbourne and Brisbane. The work we do in Canberra with the Australian Federal Government is the core of our Australian business. In developing our submission we have drawn upon this combination of global and local expertise and in light of a specific question in the issues paper around biometrics, have focused a proportion of our comments in this area.

Submission to the Development of a National Aviation Policy Statement

The aviation landscape

2007 was a busy year for Australia's international airports, with the number of international passengers arriving and departing from Australian airports rising 6% to 22.8m¹. Consistent with global trends, this growth is likely to continue, with some forecasting that passenger numbers will double within just two decades, reaching 228m air passenger movements through Australian airports by 2025-26.²

Such growth brings opportunity and challenge in equal measure. On the one hand, if Australia is to meet the national imperative of national productivity and growth, continued inward investment and increased, targeted migrant intake, then the airport infrastructure, already operating near to peak capacity will require considerable development. At the same time, the broader security climate is an evolving one, requiring ongoing monitoring and evaluation to ensure that response measures are appropriate and also responsive to passenger expectations. In Australia, the recently established Aviation Security Screening Review Advisory Group will go a long way to address this requirement.

Globally, the transport sector generally and aviation in particular are dealing with a number of key issues - rising oil prices, industry consolidation, changing security environment, the technology revolution, environmental impacts and air traffic control issues. As an example, one of the key issues that the industry is grappling with is the global standardisation of aviation security regulations, as airlines respond to differing security regulations at each international hub. Intermodal transport is also a key issue, with closer integration required between air, land and sea transportation which has implications for a whole range of regulatory, competition, security, safety and other issues.

The very function of an airport as a processing hub is changing. Passenger preferences and technology advancements are creating opportunities for passengers to 'self manage' much of their own check-in through web and kiosk applications. In turn, this is having a significant impact on the information technology (IT) systems needed to support them, with greater demand for the integration of disparate IT systems including the new passenger self service technology.

As direct human contact is increasingly reduced in passenger processing, greater emphasis is being placed on the technology in place to support the new processes, with cost efficiency and security standards compliance becoming paramount. This places an increasing onus on government not just to set benchmarks and expected outcomes, but also to more actively monitor and enforce those outcomes when necessary, particularly in relation to security and safety, as well as competition and ownership.

Technology innovations in the aviation sector continue to evolve rapidly. For example, the world's 3.2 billion mobile phones could be transformed into indispensable travel tools within 5 years³. Mobile phones could hold boarding passes, baggage tracking information and payment data, and enable a truly paperless travel environment, in a way that is much more convenient to the user. Such innovations bring additional benefits, for example, during a trial at Manchester airport in the UK, redemption of vouchers sent to passengers' mobile phones resulted in 45% higher spending amongst them compared to other airport shoppers who weren't sent the tokens.

¹ International Scheduled Air Transport, 2007

² Air passenger movements through capital cities to 2025-26, 2008

³ 'Airline' – 19 June, 2008. 'Digital travellers' could save airlines \$600m

Submission to the Development of a National Aviation Policy Statement

RFID (Radio Frequency Identification) is another technology that has the ability to create significant change in the airport environment, for example, enabling better tracking of not just assets but also passengers (via baggage tags or registered traveller cards) within an airport environment. While it may sound far fetched, such capabilities could be a valuable means of avoiding large scale airport evacuations for security purposes, and worthy of exploration of their merits.

Today's aviation environment is complex, challenging and heavily technology dependant. These attributes will only intensify as passenger numbers continue to grow. The challenge for government will be to establish benchmarks and outcomes that the industry must meet to ensure Australia's aviation infrastructure is appropriate for the increasing demands placed upon it. There is also a growing need to more actively monitor and enforce those outcomes when necessary, particularly in relation to security and safety, as well as competition and ownership.

Nationally consistent security standards

The provision of security and other common airport services is a challenging task in a complex and changing environment. With multiple stakeholders, from airport operators to government departments involved in the process, it is difficult to ensure a consistent level of service across airports. Some disparities are to be expected within any cost effective risk management approach, including the degree to which an airport is a gateway to national or international passenger movement. However, in a changing security landscape this requires close and continuous monitoring to ensure that risks are being adequately managed.

In our view, there are emerging inconsistencies in the national handling of passengers and baggage which should be closely examined.

Under current arrangements there are two primary areas of inconsistency emerging. Firstly passengers are screened to a different standard to their bags. Secondly, airports and airlines impose different security screening processes in regions compared with major gateways.

The current regulatory model requires airport operators to be responsible for security. However, airport operators represent a broad range of different government and commercial entities; from Macquarie's operations at the major airports to local councils at regional airports. Given this disparate ownership, airport operator's function largely independently of each other, with little consistency of security service delivery across the country.

Moreover, while individual airlines take some steps themselves within their own facilities, these are based largely on commercial throughputs of passengers – the more cost effective certain security measures are for a particular location, they are more likely to be considered for use there, and correspondingly not in others.

Therefore, in addition to growing disparities in our national security standards, there is a disconnected approach being taken to investments around the country. While process, technology and budgetary economies of scale could be realised, these are not feasible within the current framework. The challenges evident now will only increase as the number of passengers continues to grow.

Submission to the Development of a National Aviation Policy Statement

Recommendation 1: We recommend consideration of a more nationally standardised approach for the delivery of key security and other critical airport services

As mentioned, in today's security environment, it is paramount to maintain highly robust and consistent aviation security standards in a way that ensures continued public confidence and trust. This also needs to be done in a way that is cost competitive for airports and airlines and not cost prohibitive for the travelling public.

With discrepancies emerging under the present national framework, and issues of cost driving security expenditure, we believe consideration now needs to be given to alternative models of delivery.

In making this recommendation, we recognise that national settings favour an outcomes-based approach when it comes to aviation security – that being to define the desired outcome and allow airport operators and users to implement the system that best suits their assessment of the risk and their particular circumstances. With the imperative that consistent national security standards bring, we believe there is a case for government to mandate more uniform outcomes in certain specific areas, and facilitate the use of collective purchasing power to determine an appropriate set of solutions that drive economies of scale, for the government, for airlines and for airport operators.

The approach need not be prescriptive nor require the government to become solely responsible for aviation security, but would introduce a framework for more consistent service delivery based on risk assessment and outcome principles, with recognition that each airport is different and needs to be carefully assessed.

Alternative models are in use internationally. We believe there are particular lessons to be learned from the Canadian model introduced by CATSA (Canadian Air Transport Security Authority)

CATSA oversees passenger screening and management of card access to restricted areas. These responsibilities, carried out by third party private screening companies, are managed by CATSA which sets service level agreements for the specified security and service parameters. CATSA is funded by the Canadian Government, supplemented by an 'Air Traveller Security Charge.'

The CATSA model has introduced consistent service delivery where there was none previously, bringing standardisation to all areas of transportation security.

The model has enabled a significantly lower per-passenger management cost at Canada's 80 airports as well as other benefits including implementation of modern standard technology, best practice recruiting, training and supervision, customer-focused, high-quality motivated staff and innovative and cost effective operations.

We see a similar opportunity available in Australia perhaps through an evolved role for CASA, to provide consistency of service delivery, common technology in specific, limited areas of security, and an enhanced traveller experience while at the same time generating efficiencies in human capital and value through uniform processes and economies of scale.

Submission to the Development of a National Aviation Policy Statement

This would not be a return to centralisation, but more a hybrid model where airlines and airports retain the responsibility for implementation and the costs associated with these, but to a common standard and a narrower set of responses pre-determined by government to maintain greater uniformity.

Recommendation 2: We recommend consideration is given to the introduction of 100% checked baggage screening

While current security screening arrangements do not require 100% screening of all checked baggage carried on domestic flights, we recommend that a standard be considered that requires 100% screening of checked baggage at all domestic airports.

We believe that the current scenario where passengers are screened at 40 airports but baggage is only screened at 11 airports creates an unnecessary security risk for the traveling public.

The key driver for this measure is to provide an enhanced level of security for the traveling public.

Biometric Technology

The Government issues paper 'Towards a national aviation policy statement' released April 2008 posed the question: "Biometrics are an effective way to manage access arrangements at airports and an improvement on current practice. Is there value in introducing biometrics into Australia's airports for people working there?" We believe that there are a range of ways that biometrics can improve airport and aviation operations. In particular, biometrics represent an opportunity not just for improving current practice for airport workers, but also for improving elements of passenger security and passenger facilitation. The following information is provided to help inform your deliberations.

Biometrics, a technology that confirms a person's identity by checking their unique physical characteristics such as their iris, fingerprint or voice pattern, can be applied to security in both the public and private sectors and is used by airports, banks and other institutions. Biometric identification and verification has been implemented more widely in the aviation industry than in many other industry sectors.

As issues surrounding the validation of an individual's identity become increasingly prominent, biometrics represent important capability areas for enhancing airport and aviation security, whether validating traveller or airport worker identities. Air travel is also a natural test bed for biometric technology, and successful case studies from biometric enabled implementations in Schipol and London Heathrow airports have encouraged other airports to undertake trials.

One of the drivers for biometric solutions is the fact that documents such as home printed boarding passes can change owners or be altered easily, so a secure link must be established between the individual and the document that provides positive identity verification.

At present, governments internationally are implementing biometrics at the border and within departments and agencies, in terms of access control (airport environments, immigration and checkpoint facilities) as well as online or network infrastructure security (the use of biometric logons to computer systems).

Submission to the Development of a National Aviation Policy Statement

Increasingly in the future, we see biometrics being introduced for passenger check-in and boarding, as a general security requirement for travel. In international travel, the use of biometric technology could reduce 'boarding card swaps', a fraud risk that has the potential to occur right now with boarding cards exchanged at foreign airports between legitimate holders and individuals seeking illegal entry into Australia, individuals who then destroy all forms of ID on the flight to Australia and claim asylum on entry. The lack of ID means they can't be deported on entry and have to be processed as asylum seekers.

Biometrics also has a role to play in enhancing the traveller experience. In 2005, the International Air Transport Association (IATA) launched an initiative called Simplifying Passenger Travel (SPT). The program's objective is to generate a more passenger-centric approach, replacing repetitive security checks of travellers and their documents with biometric enabled technology. Additionally, the introduction of biometric border-crossing systems at a number of European airports over the last few years has shown that biometric technology can improve security outcomes and overcome barriers such as technology and cultural resistance.

The use of a person's physical characteristics to confirm their identity has traditionally been discussed in terms of privacy. However, as Unisys research has shown, community attitudes towards privacy are evolving. Security today is seen as not just a way of life, but a pre-requisite. The Unisys Security Index⁴ showed that 98 per cent of Australians are prepared to use a photograph to establish their identity, while 75% are happy to have their fingerprints taken and 69 per cent would agree to iris scans. This is further elaborated below.

Recommendation 3: We recommend consideration of a biometric enabled Aviation Security Identification Card (ASIC)

One particular application for biometric technology within the airport environment is to validate the identity of individuals authorised to access airport 'sterile' areas and their authority to perform a particular task, such as driving a baggage truck or fuel tanker.

A biometric enabled ASIC card, for example a fingerprint and/or iris scan, would increase the level of confidence that the person carrying the card is the approved user and could also remove the need for 'sterile' area access points to be physically manned.

To safeguard privacy, the ASIC card biometric wouldn't need to be stored on a central database, instead the data would be stored on the card itself, additionally utilising PKI (public key infrastructure) authentication. This technology could be applied to the current 90,000 ASIC card holders to further strengthen the provision and use of the card.

Unisys is playing a role in the implementation of a similar solution for the Port Authority of Los Angeles, US, essentially to design and manage an identification and access control system, using smart card and biometric technologies, to identify workers who require access to restricted areas in the port. The smart card will include a biometric component - a fingerprint template - and a digital photograph that will integrate seamlessly with each operator's access control system and allow port facility security officers to identify all workers granted access to restricted areas.

⁴ Research released in September 2006

Submission to the Development of a National Aviation Policy Statement

According to TSA, workers enrolled in the pilot would present a card to a biometric-enabled reader and place a finger on a reader at all pedestrian and vehicle ingress locations. The readers will compare the cardholder's fingerprint to the stored biometric template and automatically grant or deny access, as well as notify facility security officers of any incidents.

The project is part of the federal Transportation Worker Identification Credentials (TWIC) program, a joint effort of the U.S. Transportation Security Administration (TSA) and the U.S. Coast Guard to help secure the US's maritime transportation system. It was established under the Maritime Transportation Security Act of 2002 which calls for a comprehensive, consistent security program for the nation's ports to identify and deter threats.

In addition, over the past few months, Unisys has introduced a vascular scanning system for 4,000 workers at the Port of Halifax in Canada. This uses an infrared scan of the back of the cardholder's hand which is embedded in a smart card which also includes the holder's photograph.

This vascular image, which is recognised by a non-invasive infrared sensor, identifies the card holder when they present the card and place the back of their hand in the scanner. Verification is instantaneous and is achieved when the blood flow pattern of the holder's hand matches the pattern of the scan stored on the card.

The system is used to validate identity and to validate authorisation to carry out a specific task or operate a specific piece of machinery.

Unisys is working on a similar initiative in Canada with The Canadian Air Transport Security Authority (CATSA). The project's objective is to supply, integrate and manage a new identification management system, using fingerprint and iris biometric technology to verify the identities of airport workers at 29 airports throughout Canada.

The new system will replace the existing application used in CATSA's Restricted Area Identification Card (RAIC) system. The RAIC system enhances aviation security by verifying the identities of airport workers via biometrics and ensuring that only those workers with security clearance are permitted to enter restricted areas. It also allows CATSA to update the security clearance status of all 100,000 airport workers instantly at all airports across the country.

The system uses contactless smart cards, fingerprint and iris readers located at entry points to restricted areas and enrollment equipment which communicates with the airport's access control systems. Airport workers scan smart cards in readers, which extract the biometric data. The user then provides a fingerprint or iris scan which is matched against the data on the card.

Recommendation 4: We recommend consideration of identity verification for all Australian domestic airline travel

In the current domestic check-in process, passengers and their carry-on baggage are screened before being allowed airside or to board the plane, but there is no physical identity verification of passengers checking in via the web or a kiosk. In situations such as the recent Brisbane incident⁵, errors can lead to massive dislocations, inconvenience and delay. There is also the issue of security – there is no guarantee that the person who checks in is the person who boards the

⁵ April 2008 nine people inadvertently bypassed x-ray checks in the Qantas terminal at Brisbane domestic airport, causing its evacuation and considerable flight delays.

Submission to the Development of a National Aviation Policy Statement

aircraft. This is an issue if the traveller is on a watch list or a 'person of specific interest' to the AFP for example.

The identity validation could be as simple as a photo ID, or, in a more secure mode, utilise a biometric such as a fingerprint or iris scan – both would create a more secure process than currently exists. Hbox scanning technology⁶ currently under trial in the US undertakes face and iris scans as passengers walk beneath readers mounted at key points in the airport screening process, in trials processing upto 50 passengers a minute.

Another option would be to integrate identity verification with the new 'smart' driver licence due for initial rollout in Queensland. The data collected for this licence (which includes biometric identifiers) could additionally be used to support passenger identification.

This process would bring multiple benefits – an enhanced level of security, greater peace of mind for travellers and confirmation of identities for everyone airside in the domestic terminal. It will also mitigate security breaches such as the Brisbane incident by ensuring a positive confirmation of who is in the terminal and confirmation that the passenger name on the boarding pass matches the identity of the traveller.

Acceptance by travellers may also be higher than previously expected. Unisys research⁷ has shown that in the interests of enhanced domestic aviation security, Australians are prepared to have all bags electronically tagged for monitoring (91%) arrive earlier for extra screening (84%) participate in a travellers identity scheme (68%) and provide a fingerprint or biometric to airlines (71%). More generally, nearly all Australians (98%) say they would be happy to use extra techniques such as photographs and fingerprints to prove who their identity. The most popular form of secure identity verification was a photograph with 84% support. All other forms of identity verification (including fingerprints, iris scans) were supported by over two thirds of the population.

Recommendation 5: We recommend consideration of incident management processes in airports for situations where passengers evade the security screen which enables them to be identified and recalled without evacuating the airport terminal

The aforementioned incident at Brisbane airport has shown that when a traveller passes through the security screen checkpoint without being screened, whether by default or design, there appeared not to be a clear plan in place to either confirm their identity or locate them in the airport, with the result that the only option is to evacuate the airport to eliminate any potential risk to travellers or infrastructure.

Technology has a role to play in addressing this challenge, for example, RFID is an automatic identification technology that stores and remotely retrieves remotely data using devices called RFID tags. As an example, Copenhagen Airport is testing RFID passenger tracking to improve performance and allow direct communication with passengers, making the contact more reliable and reducing the terminal noise level. It's unlikely that the RFID tag would be placed on the

⁶ HBOX is iris-at-a-distance scanning technology developed by Global Rainmaker Inc. (GRI)

⁷ Unisys Security Index 2006

Submission to the Development of a National Aviation Policy Statement

passenger themselves, more likely it would be embedded in a baggage tag, boarding pass or registered traveler card.

Such a solution, combined with the confirmation of passenger identity via photo ID or a biometric identifier would remove the need to evacuate the airport, instead allowing the individual to be identified and located within the airport.

We are not aware of the processes in place at all national and regional airports. However, if the Brisbane incident was indicative, we believe that consideration should be given to such initiatives that provide increased levels of security and minimise disruption to the traveling public.

Passenger facilitation

There is a growing recognition within the aviation sector internationally that passenger transit through airports has become a frustrating, slow and cumbersome experience – this is despite some early innovations in the field such as self service check-in. This is a consistent picture around the world, an inevitable outcome of the enhanced security measures put in place post 9/11 and subsequently, as well as the sheer volumes of passengers that the sector deals with today. The result is that airports have become stressful environments, a condition which is at odds with industry service and passenger satisfaction goals. Around the globe, airport operators, regulators and other stakeholders are seeking ways to facilitate smoother airport passage.

In the past, approaches to aviation security screening have traditionally been based on a mindset of common and single processes for all passengers, regardless of their potential risk. The advent of security technologies today enable you to implement consistent standards of security with some pre-screening of some passengers who meet certain pre-qualification criteria – such as frequent business travellers.

At the same time, passengers themselves are increasingly demanding of faster and more convenient passage – whether they are travelling for business or pleasure. What is not yet widely recognised, however, is the degree to which the travelling public is willing to participate in the process in a more active way, if it brings a benefit in terms of security and convenience. This in turn is opening up new areas for government and industry to work together in the sector.

It is worth restating that community attitudes towards security and privacy are evolving and it is important that any national policy, regulatory and other settings continue to keep pace with this change.

One of the strongest drivers of attitudinal change is the vastly different environment in which we live today. A whole range of international, national and local factors have radically altered the context in which we live work and play. For one, people think about security much more broadly than they once did, and are much more demanding of security in many dimensions⁸ Security today is seen as not just a way of life, but a pre-requisite, and as the security environment has changed, so have the measures needed to counter it. Alongside security, people also want

⁸ Since launched in June 2006, the Unisys Security Index has shown consistently that Australians are concerned about a range of security issues – personal, internet-related, national and financial.

Submission to the Development of a National Aviation Policy Statement

convenience – to do their banking online, to travel easily – and with this comes a willingness to participate in security by providing personal information.⁹

At the same time, Australians are more concerned about misuse of their personal information than any other security issue.¹⁰ Clearly privacy remains important to most people. However, today people are willing to forgo some degree of privacy if it means that their personal or financial information, or their personal safety, will be better protected.¹¹ Additionally, younger generations are demonstrating significantly different attitudes towards privacy related issues than their older counterparts, including privacy generally and in an online environment.¹² Australians also send mixed signals when it comes to protecting their personal information, with many still not taking even simple steps to protect themselves.

In our view, attitudes towards security and privacy are evolving such that traditional tradeoffs between security, privacy and convenience are reducing in relevance – today each are seen as necessary and coexisting factors in any security response.

Recommendation 6: We recommend consideration of a ‘Traveller Identity’ initiative designed to provide an enhanced travelling experience for frequent international and domestic travellers

We believe that the area of ‘traveller identity’ presents a number of opportunities for the Australian government and industry to work together for the benefit of the passenger experience, consistent with trends around the globe.

A ‘traveller identity’ program would provide a number of benefits to the domestic and international traveller, identifying passengers who pose a minimal security risk, and then providing those passengers with expedited passage through the airport. For domestic travel, the introduction of identity verification would be a prerequisite for a traveller identity initiative.

Similar initiatives are already in operation in other airports around the world. In the United States, the TSA (Transportation Security Administration) has introduced a ‘Registered Traveller’ scheme at a number of domestic airports. Under the guidelines, passengers pay a fee and submit to a background check to enroll in the program. Those who pass the background check are then issued a smartcard for use at the security checkpoints of participating airports. Registered Travellers benefit by using a dedicated security lane while regulators benefit from a more complete profile and record of these participants. In order to prevent a terrorist with a clean background from compromising the system, the US Transportation Security Administration (TSA) requires that registered travellers undergo the normal TSA screening (baggage x-ray and personal metal detector), as well as clearance via the Registered Traveller kiosk checkpoint. This program was implemented by Unisys.

⁹ Research conducted for Unisys in 2006 by The Ponemon Institute, a leading independent firm that specialises in privacy and security research found convenience the leading reason for biometrics support.

¹⁰ The Unisys Security Index has consistently found that concerns about unauthorised access to or misuse of personal information is the issue that concerns Australians the most.

¹¹ Since we launched the Unisys Security Index in mid 2006, we have consistently seen a lower level of concern amongst younger age groups across a number of security and privacy related issues, including lower levels of concern regarding privacy protection and lower levels of concern across the internet category of issues (shopping and banking online + risks associated with viruses and unsolicited emails).

Submission to the Development of a National Aviation Policy Statement

Sciphol airport in the Netherlands was one of the first airports to introduce a biometrics enabled 'traveller identity' program which allowed travellers to pass a national border without going through passport control. The program, established in 2001, now has in excess of 30,000 members using the scheme.

London Heathrow Airport used biometric applications for a trial conducted between January and June 2007. The trial captured traveller fingerprints at check-in which enabled the airport to replace manual identity checks in the screening area with an automated gate using a fingerprint scanner and boarding card reader. An additional benefit to the airline was the identity verification provided the boarding confirmation to allow the ground crew to load the passengers baggage. Passenger feedback suggested that the reduction in security line waiting times and perceived security gains outweighed any other concerns they had.

Closer to home, as you are no doubt aware, Qantas has been trialing a program at Melbourne airport using 3D security screening, a technology that uses millimetre waves, or radio waves, to scan the body and identify any concealed objects being carried by a passenger. The process is voluntary at this stage, but the airline intends to roll out the technology across all airports and possibly replace metal detectors.

As public discussion on the Qantas example has shown, critical to realising the potential benefit is a dialogue with the public impacted and a clear understanding of the traveler value proposition. They have personal preferences on some security measures over others and it is important that these are taken into account in the planning and implementation process.

In Australia, Unisys is currently developing and implementing an identity authentication solution for the Australian Department of Immigration and Citizenship designed to strengthen Australia's borders using facial recognition and fingerprint scanning technology.

Inter agency co-operation

Recommendation 7: We recommendation exploration of ways to generate greater inter agency communication & co-operation

Post 9/11, there has been greater focus globally on domestic and international inter-agency information sharing in the ongoing fight against terrorism and Australia has a good track record in this area to date.

Within an airport environment, there are multiple government agencies and commercial enterprises involved in airport operations, operating in complex and ever-changing conditions. The closer the coordination between these disparate organisations, the greater the likelihood that their combined knowledge will lead to the prevention of security breaches.

For reasons of governance, technology, culture and cost, it can be difficult for appropriate sharing mechanisms to be put in place. However, we would encourage all stakeholders to continue investigating means to enable greater solution and information sharing and therefore enhance the security environment.

Submission to the Development of a National Aviation Policy Statement

Airport operations

Airports, as vital nodes in the system of worldwide air transport, have traditionally simply been defined as infrastructure. But driven by economic necessity, they have evolved to become the complex and burgeoning commercial enterprises we see today. That said, the vital need for precise and safe operations is often at odds with profitability or attempts to optimise the cost of operations. And unlike other commercial enterprises however, airports also have a comparatively higher imperative in terms of national security. For this reason, we believe it is valuable making a number of general remarks in terms of infrastructure planning and preparedness.

These contradictory demands have created critical need for greater efficiency at airports. Where in other industries this equates to leveraging emerging technology to optimise process design, airports have additional complex requirements. Airport operators are challenged to maximise structure capacity while simultaneously enhancing the customer experience, cope with growing passenger numbers and growing revenues, for example via retail sales.

Airport challenges have never been more wide-ranging and consequential, and the price of wrong decisions has never been so great. Most business processes depend on rapidly changing and evolving information technology, and only flexible application services can make an airport agile enough to follow these constant changes in the industry.

Consequently, airport managers need to shift a greater percentage of their IT investment to innovation, as opposed to continued maintenance and further integration of expensive, complex and increasingly dysfunctional legacy systems. IT investment decisions are no longer tactical. They need board room support as they become ever more strategic.

Based on clear business decisions and priorities, each airport CIO should review and renew the IT infrastructure and application landscape plans. In the context of the government's plans to attract greater inward investment and migrants, this is particularly important for Australia's network of international airports.

Never has the environment for change been better than it is today. Various industry initiatives such as IATA's 'Simplify the Business'¹³ and new emerging technologies provide added incentive to restructure and update. Many alternatives to existing legacy IT architecture exist and while it is true that change involves risk, IT vendors have mitigated this risk via the use of sophisticated tools and base concepts.

Green issues such as the reduction of carbon emissions have also moved onto the airport IT agenda as well as being at the forefront for the industry in general. IT has a role to play in this space, for example airlines and airport authorities are increasingly using powerful business analytics tools to provide fuel burn data to determine the most efficient routes and fuel consumption rates. An example of this is the platform operating at Airways New Zealand which has reduced the time planes spend circling Wellington airport whilst waiting to land by 10 hours a month, saving 456 tonnes of fuel per annum. A similar initiative is under trial with Airservices Australia in Brisbane.¹⁴

Emerging technologies such as the bar-coded boarding pass in combination with self-service concepts allow for greater efficiency and throughput in terminals. This innovation will likely have

¹³ IATA (International Air Transport Association) launched its industry-wide 'Simplifying the Business' initiative in 2004 to remove complexity, enhance customer convenience and lower industry costs

¹⁴ Source: Australian Financial Review 'Squeezing value from every drop', 17 June 2008

Submission to the Development of a National Aviation Policy Statement

a far-reaching impact on airport planning, allowing the capacity of terminals and baggage handling systems to be maximised and additional capacity gained by smarter use of existing space and new technology, whilst reducing costs.

RFID is another technology that will provide enhanced capability in this area. If an airport strategically places actuators, (e.g. RFID antennas) and movable objects (e.g. passenger baggage) are equipped with RFID tags, close monitoring of people and assets becomes possible.

While we make no direct recommendation in this area, we would underline the ongoing importance of technology, innovation and process efficiency in Australia's airport infrastructure. Airport efficiency is directly linked to our ability to support the predicted growth in passenger numbers, enabling the government's plans to attract greater inward investment and migrants into the Australian market.

Concluding remarks

In conclusion, I would like to reinforce our commitment to the Australian Federal Government market. We attach great importance to this Review and the process that the Australian Federal Government has initiated, and would be very happy to expand on any of the issues raised in this submission.

Yours sincerely,



ANDREW BARKLA
Vice President and General Manager
Unisys Asia Pacific