GOVERNMENT RESPONSE TO THE REPORT OF THE PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT:

Inquiry into the Adequacy of Aviation and Maritime Security Measures to Combat Serious and Organised Crime

Table of Contents

1. Introduction

This document details the Australian Government Response to the recommendations made by the Parliamentary Joint Committee on Law Enforcement (PJC): *Inquiry into the Adequacy of Aviation and Maritime Security Measures to Combat Serious and Organised Crime*. The Government thanks the Committee for its inquiry and the report.

In 2008, as a part of the Prime Minister's inaugural National Security Statement, the Australian Government recognised serious and organised crime as a national security threat and a growing national challenge. In response, the Australian Government launched the Organised Crime Strategic Framework in 2009 which establishes a comprehensive and coordinated response to target organised crime wherever it exists—including at the border.

The Australian Government's approach to border control and law enforcement at airports and seaports is a multi-layered and cooperative effort between Commonwealth, and State and Territory agencies, as well as partnership with the aviation and maritime sectors.

At both airports and seaports, the Australian Customs and Border Protection Service (Customs and Border Protection) is responsible for protecting the safety, security and integrity of Australia's border through a wide range of regulatory and enforcement powers. Key functions include preventing and intercepting illegal movements of people and goods (such as illicit drugs and firearms) across the Australian border. In undertaking this role, Customs and Border Protection primarily works with a range of key Commonwealth partners, including the Australian Federal Police (AFP), the Australian Crime Commission (ACC) the Department of Immigration and Citizenship and the Australian Quarantine and Inspection Service.

The Office of Transport Security (OTS) within Department of Infrastructure and Transport (DIT) provides the Australian Government with policy advice and regulatory oversight of preventive transport security in the aviation, maritime, offshore oil and gas and air cargo sectors. This is achieved through the *Aviation Transport Security Act 2004* (ATSA), the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA), and associated regulations. The approach to preventive security embodied within the ATSA and the MTOFSA focuses on the protection of transport assets and those who use them.

OTS follows a risk-based, outcomes-focused approach to regulation through consultation with industry and international engagement. OTS works with industry to ensure compliance with the law and regulations by effecting changes in industry participant behaviour towards their regulatory obligations. Within the international context, OTS contributes to the achievement of Australian Government outcomes on transport security by working closely with the International Maritime Organization and the International Civil Aviation Organization, and by subscribing to international treaties and participating to international forums.

AusCheck is a branch within Attorney-General's Department (AGD) responsible for undertaking background checking for the ASIC and MSIC schemes. AusCheck applies a consistent interpretation of statutory requirements, coordinates criminal and security checks

on ASIC and MSIC applicants (and immigration checks where requested) and notifies the relevant bodies on the outcomes of these checks.

The AFP is the primary law-enforcement agency at Australia's 11 major airports through its Unified Policing Model. These airports are Adelaide, Alice Springs, Brisbane, Cairns, Canberra, Darwin, Gold Coast, Hobart, Melbourne, Perth and Sydney. The AFP's role will be strengthened through the move to "All-in" policing at major airports. Law enforcement at regional Australian airports is primarily the responsibility of the States and Territories.

The AFP's key tasks in the aviation environment are targeting organised crime, deterring acts of terrorism, providing a uniformed policing presence, providing a first response to acts of terrorism and emergency incidents, collecting and analysing aviation intelligence and conducting investigations. In undertaking this role, the AFP works closely with airport operators and airlines in addition to Commonwealth, State and Territories agencies.

The States and Territories retain the primary responsibility for enforcing state offences and criminal law at Australian ports. The AFP has the primary responsibility for investigating federal crime in the wider maritime environment. There are arrangements in place to ensure close cooperation between Commonwealth, and State and Territory agencies.

The ACC, as the national criminal intelligence agency, plays an important role in supporting the law enforcement community and the broader government, including at Australia's airports and seaports. This includes the provision of a range of strategic, tactical and operational intelligence products which provide partner agencies with the context to understand serious and organised criminal threats to Australia. In undertaking this role, the ACC utilises its national criminal intelligence holdings, coercive powers and a national legislative and organisational framework that facilitates cooperation on a range of operational outcomes.

2. Response to Recommendations

2.1. Expanding the Scope of transport security legislation

Recommendation 1

The committee recommends that the scope of the Aviation Transport Security Act 2004 *and the* Maritime Transport and Offshore Facilities Security Act 2003 *be widened to include serious and organised crime in addition to terrorist activity and unlawful interference.*

Noted

The Commonwealth Organised Crime Strategic Framework states that industry "has a key role in understanding its environment and identifying potential opportunities for organised crime exploitation". The Government's approach to organised and serious crime is based on "preventative partnerships" between government and industry participants.

The ATSA and MTOFSA, administered by the Department of Infrastructure and Transport, are designed to provide a national regulatory framework for the aviation, maritime, and offshore oil and gas sectors. They require industry participants to prepare transport security plans and implement risk based preventive security measures aimed at facilitating transport by reducing the risk of unlawful interference with transport systems under their control. Any amendments to the ATSA and MTOFSA have always been developed in a way that minimises the impact on industry, in line with the Government's objective of achieving an efficient, sustainable, competitive and secure transport system.

Noting the above, it is proposed that the Attorney-General's Department, in close consultation with the Department of Infrastructure and Transport, establish an aviation and maritime industry forum to examine options for organised and serious crime prevention at Australian airports and seaports in partnership with industry. This will include examining legislative change options, such as the potential to enhance powers under the *Customs Act 1901*, in the context of working with industry to address serious and organised crime in the aviation and maritime border environments. This would be informed by ACC risk assessments relevant to organised and serious crime in Australia's airports and seaports.

2.2. Law enforcement on airports and seaports

Recommendation 2

The committee recommends that security at major airports be undertaken by a suitably trained government security force.

Not agreed

This matter was considered by Government in December 2009 as part of *Flight Path to the Future: National Aviation Policy White Paper*. This document confirmed that the current industry led and government regulated model provides an "effective, efficient and sustainable security service, notwithstanding evolving threats, increased security requirements, and increases in domestic and international aviation traffic".

A more centralised model was not supported on the grounds that a government agency screening model would be overly prescriptive, more expensive and less efficient than current arrangements.

The Government continues to work with industry to improve the current system through improved industry guidance, enhanced technology and better training.

Recommendation 3

The committee recommends that joint maritime taskforces, mirroring the functions of the Joint Aviation Investigation Teams and Joint Aviation Intelligence Groups in the maritime sector be established in every state and the Northern Territory. These taskforces should include officers of the Australian Federal Police, state or territory police, the Australian Customs and Border Protection Service and the Australian Crime Commission.

Noted

The objective of this recommendation is already being achieved at Australian ports through existing cooperative arrangements between the specified agencies to address security and criminality at the waterfront. Customs and Border Protection has also established a Maritime Intervention Strategy to help detect, deter and disrupt criminal activity and to improve its presence in the port environments through a range of law enforcement functions, targeted operations and campaigns.

Currently, joint multi-agency taskforces are established as needed to deliver targeted operational responses against identified criminal threats. Due to the unique nature of the maritime environment and need for law enforcement responses to be flexible and responsive to direct intelligence, the more rigid model employed in the aviation environment through the Joint Aviation Investigation Teams and Joint Aviation Intelligence Groups is not supported.

However, the Commonwealth will continue to consider whether there are other options to strengthen existing arrangements.

Recommendation 4

The committee recommends the formation of a Commonwealth maritime crime taskforce that would act as a national Australian Federal Police led "flying squad", responding to specific intelligence and also conducting randomised audits of maritime and seaport security.

Not agreed

This recommendation largely reflects existing AFP practices in relation to law enforcement and investigations in the maritime environment. These activities also involve a range of Commonwealth, State and Territory agencies.

However, a role for AFP in conducting audits of maritime security is not supported as the AFP does not have sufficient expertise in this area.

Recommendation 5

The committee recommends that the Attorney-General's Department conduct a review of current information sharing arrangements between law enforcement agencies and private organisations in the aviation and maritime sectors.

Agreed

AGD will lead this review in consultation with the AFP, ACC and Customs and Border Protection.

This recommendation is consistent with the Organised Crime Strategic Framework's objectives of strengthening information sharing between law enforcement agencies and working more closely with industry. There is a range of existing partnerships and information sharing practices between law enforcement agencies and with the private sector that the Commonwealth will continue to explore opportunities to improve. This will include additional opportunities for enhanced intelligence sharing between law enforcement agencies and the private sector where appropriate.

2.3. Identity confirmation for domestic passengers

Recommendation 6

The committee recommends that the Crimes (Aviation) Act 1991 *be amended so as to create a new offence of deliberately travelling under a false identity.*

Agreed

A specific offence of intentionally travelling under a false identity would provide a further tool for combating terrorism and organised crime in the aviation environment. AGD will work with the AFP and DIT to develop an appropriate offence.

Recommendation 7

The committee recommends that it be made a legal requirement to provide photo identification confirming passenger identity immediately prior to boarding an aircraft.

Not agreed

The recommendation as specified is not supported, particularly the requirement for all passengers to provide photographic identification.

The Government acknowledges the need to strike the right balance between facilitating passenger travel at airports and minimising the risk of serious and organised criminal activity. Industry stakeholders have also expressed concerns that an approach such as the one recommended may lead to delays in passenger facilitation (especially at large airports that are close to reaching capacity) and additional costs to industry and the travelling public.

The Government will utilise the aviation industry forum to be established by AGD to examine options for serious and organised crime prevention to further consider the benefit, and the impact on industry and the public, of creating an obligation for individuals of concern to provide appropriate identification prior to boarding an aircraft. Under current arrangements, it would be ineffective and impractical for such activities to be conducted by airport check-in staff who are not trained to recognise fraudulent documents and have no law enforcement powers.

It is also not feasible for a government official, acting as government security officer, to conduct identity checks of all passengers on domestic aircraft services as there is not sufficient capacity to staff each boarding gate in order to conduct identification confirmation.

2.4. Access, information sharing and customs issues

Recommendation 8

The committee recommends that the Commonwealth Government review the technical and administrative requirements necessary to facilitate the effective sharing of information between airlines and air cargo agents and law enforcement agencies and the Australian Crime Commission Fusion Centre for the purpose of enhancing aviation security and law enforcement activities. The review should include research into technical requirements for such a scheme, the costs involved and any relevant statutory or other barrier to the sharing of such information. The findings of the review should be reported to the Australian Parliament.

Agreed

The AGD will lead this review in consultation with the AFP, ACC, and Customs and Border Protection.

This recommendation is consistent with the Organised Crime Strategic Framework's objective to continue to strengthen information sharing between law enforcement agencies and working more closely with industry. This work will complement the review to be conducted in response to recommendation 5 on information sharing arrangements between law enforcement agencies and private organisations in the aviation and maritime sectors.

The Commonwealth will consider options for reporting the findings of the review. As the review may contain operational sensitivities that cannot be made public, it may not be possible to report the full findings of the review to Parliament.

Recommendation 9

The committee recommends that the Australian Government provide further resources to support an increased presence for currency and illicit drug detection canine units at Australian airports.

Noted

The Commonwealth considers that current levels of currency and illicit drug detection canine units are sufficient.

The AFP is undertaking a review of whether there is need for additional canine units in the future. The AFP will also review the terminating "Firearms and Explosive Detector Dogs" Budget measure and together with Customs and Border Protection will consider whether additional resources for currency and illicit drug detection canine unit are needed.

Recommendation 10

The committee recommends that access to port security areas prescribed under the Maritime Transport and Offshore Facilities Security Act 2003 *should require verification that the Maritime Security Identification Card belongs to the individual seeking access, either through human gate operators, verification by Closed Circuit Television or any other appropriate solution.*

Noted

The DIT will assess current preventive security settings to ensure that appropriate outcomes are being met at all security regulated seaports.

The current approach in relation to seaport security is that the preventive security measures at facilities (including access control arrangements) should be commensurate to the security risk particular to the facility. A prospective "one size fits all" approach would incur unnecessary costs for industry that may not be commensurate with local security risk circumstances.

While face to MSIC checks are required at some higher risk facilities, in areas of lower risk, other security approaches, such as electronic swipe access coupled with random inspection and controls may be appropriate.

Recommendation 11

The committee recommends the development of a system that enables the confidential movement and examination of containers that increases the likelihood that trusted insiders involved in serious or organised crime are not alerted to law enforcement agency interest in a container.

Noted

Customs and Border Protection currently has the ability to employ several methods to carry out covert movements and examinations of containers.

Customs and Border Protection will continue to examine changes in the maritime environment and technological advances to enhance its ability to conduct covert operations and reduce the risks presented by trusted insiders involved in organised crime.

Although Customs and Border Protection notes that it is not possible to completely avoid surveillance by interested parties seeking to identify covert activity in the supply chain, options to reduce this visibility will continue to be explored.

Recommendation 12

The committee recommends that the Commonwealth government further invest in CCTV at airports and ports, with consideration of a number of ongoing improvements, including:

- *that CCTV cameras should be capable of producing footage of evidential quality;*
- *the continuing lead role of Customs in coordinating the monitoring of CCTV networks; and*
- *that CCTV networks should be complemented with automated number plate recognition, and/or facial recognition technology.*

Noted

Closed-circuit television (CCTV) at airports and seaports is operated by a range of businesses and government agencies for a variety of purposes which includes but is not limited to people traffic management, customs and border protection, anti-shoplifting purposes in retail areas, physical security of the facilities, and aviation/maritime security.

Customs and Border Protection installs and maintains CCTV equipment throughout Australia's eight international gateway airports and 63 gazetted seaports to assist in its border management and security objectives.

In consultation with relevant stakeholders, Customs and Border Protection has developed the *CCTV Strategic Outlook 2020*, a strategy to guide future investment in CCTV at the border. The strategy has been developed in recognition of increasing interest from stakeholders in obtaining access to high quality visual information and the need to update existing CCTV technology that is approaching obsolescence. This strategy has been endorsed by the Border Management Group which comprises a range of Commonwealth partner agencies.

The initiatives identified in the strategy are intended to be progressively implemented by Customs and Border Protection following proof of concept trials to refine business requirements, which includes sharing arrangements with industry.

Within current resource constraints, the implementation of the initiatives is being prioritised according to the business needs of individual Australian's eight international gateway airports and 63 gazetted seaports, and the level of risk presented by existing systems.

In addition to the work of Customs and Border Protection, the National Counter Terrorism Committee, Legal Issues Sub Committee CCTV Working Group is developing a national policy and strategy for CCTV regarding the production of footage of evidential quality and a Practical Guide for law enforcement and national security agencies for use when using CCTV vision in counter terrorism investigations.

Recommendation 13

The committee recommends that Customs be given the power to revoke a depot, warehouse or broker's license if it determines, on the strength of compelling criminal intelligence, that an individual or individuals are involved or strongly associated with significant criminal activity.

Noted

Customs and Border Protection recognises the importance of preventing the likelihood of criminal infiltration in the cargo process. The positions of trust placed on depot, warehouse and broker's license holders is essential to ensuring that Customs and Border Protection controls are effectively enforced and border integrity is maintained.

Customs and Border Protection is strengthening its licensing regime and has been given legislative power to place conditions on depots' licenses that can be applied on a case-by-case basis to require the provision of staff lists for assessment against intelligence holdings.

The Commonwealth considers that a more appropriate step would be to reinforce Customs and Border Protection's power to scrutinise and monitor individuals and companies involved in the licensing regime. Customs and Border Protection will examine options to further strengthen its licensing regime with initiatives such as the power to request and assess staffing data.

2.5. Changes to the ASIC and MSIC schemes

Recommendation 14

The committee recommends that the Attorney-General's Department, in consultation with the Australian Crime Commission, reviews the list of relevant security offences under the ASIC and MSIC schemes to assess whether any further offences are required in order to effectively extend those schemes to protect the aviation and maritime sectors against the threat of infiltration by serious and organised criminal networks.

Agreed

DIT and AGD, in consultation with the ACC, will review the lists of security-relevant offences to assess whether any further offences are required.

Recommendation 15

The committee recommends that the Attorney-General's Department arrange for a suitable law enforcement agency to be given the power to revoke an Aviation Security Identification Card or Maritime Security Identification Card if it is determined that a cardholder is not a fit and proper person to hold a card on the basis of compelling criminal intelligence.

Noted

DIT and AGD will consider options for developing a test that would allow a suitable law enforcement agency to cancel an ASIC or MSIC if it is determined that the card holder is not a fit and proper person based on compelling criminal intelligence. This will include options to appeal any such determination, and a suitable legal mechanism for cancelling such cards.

This policy work will be conducted in conjunction with the proposed review of security-relevant offence criteria to respond to Recommendation 14.

Recommendation 16

The committee recommends that the MSIC eligibility criteria be harmonised with that of the ASIC scheme so as to make two or more convictions of an individual for maritime security relevant offences grounds for disqualification if one of those convictions occurred in the 12 months prior to an application, regardless of whether either conviction led to a term of imprisonment.

Agreed

The DIT will assess the eligibility criteria exclusion mechanisms in the ASIC and MSIC schemes with a view to greater harmonisation if appropriate.

Recommendation 17

The committee recommends the expansion of the coverage of the ASIC and MSIC schemes to capture a greater part of the overall supply chain, including some or all of the following:

- *staff at cargo unpacking and stuff-unstuff facilities;*
- *transport workers involved in the transmission of cargo between ports, airports and other parts of the logistical chain;*
- *customs brokers that do not access port facilities; and*
- *human resource staff and management at companies with employees that currently must hold ASICs or MSICs.*

Noted

The DIT, in conjunction with the AGD and relevant portfolio agencies, will evaluate the potential security benefits of expanding the categories of people required to hold ASICs/MSICs.

Recommendation 18

The committee recommends that AusCheck and CrimTrac work together to develop a database system that enables continual assessment of a cardholder's criminal record in order to ensure that cardholders are disqualified very soon after being convicted of a relevant security offence.

Noted

While there would be many benefits to continuous criminal history checks, there are a number of technical, privacy, legislative and funding issues that need to be resolved to achieve this outcome.

AusCheck and CrimTrac, in close consultation with the States, Territories and other relevant Commonwealth agencies, will work together to explore options which allow for the ability to continually identify those ASIC and MSIC holders who are convicted of security-relevant offences that pose a threat to the aviation and maritime environments.

The Government notes that both the ASIC and MSIC schemes have mandatory self reporting requirements in place which are designed to identify those card-holders who may be convicted of a security-relevant offence in order to reassess their eligibility to hold a card.

Recommendation 19

The committee recommends that use of biometric information, particularly fingerprints, to establish a unique identifier for applicants for the purpose of maintaining an accurate database of cardholders.

Noted

The Government notes the recommendation and will consider the use of biometric information in the context of its work coordinating Australia's National Identity Security Strategy, a cross jurisdictional initiative endorsed by COAG in 2007. One of the key elements of the Strategy is enhancing national inter-operability of biometric identity security measures which is being progressed through the development of a Biometrics Interoperability Framework.

The Biometrics Interoperability Framework is intended to cover the use of biometrics across law enforcement, national security and service delivery purposes, recognising that rapid developments in biometric technologies and advancements in the capture, transfer and storage of digital information is resulting in increased take-up of biometrics across the public sector generally. The framework is exploring specification of the uses of particular biometric types, namely fingerprints and face; the manner in which biometrics information is validated, stored and shared; and the data standards applicable to achieving interoperability.

Recommendation 20

The committee recommends that the Australian Government consider the use of biometric information for the purpose of controlling access to security controlled areas in the aviation and maritime sectors.

Noted

The DIT will in close consultation with relevant government agencies and the aviation and maritime industry sectors consider potential options to introduce biometrics for the purpose of enhancing access control arrangements at Australian airports and seaports. The

Government recognises the link between this recommendation and recommendations 10 and 19.

Recommendation 21

The committee recommends that AusCheck establish memoranda of understanding with the Australian Federal Police and other key law enforcement and intelligence agencies in order to allow the timely provision of information held in the AusCheck database to those agencies.

Agreed

The Government supports the recommendation and actively promotes information sharing within the law enforcement community.

AusCheck already provides law enforcement and intelligence agencies access to its database for law enforcement and national security purposes within the parameters set down in the *AusCheck Act 2007*. AusCheck publishes publicly accessible guidelines that govern who can receive information from the AusCheck database, the purposes this information can be used for, and the process for requesting this information.

AusCheck has developed and entered into a number of Memoranda of Understanding (MoUs) with a variety of relevant law enforcement agencies, including the AFP. These MoUs ensure that access to the AusCheck database appropriately addresses the needs of the law enforcement agencies, including the need for fast response times, while conforming to the requirements of the AusCheck legislation and guidelines.

AusCheck regularly reviews its MoUs and is currently engaged in developing new MoUs with additional Commonwealth authorities that have functions relating to law enforcement. AusCheck is exploring the possible extension of its MoUs to incorporate the development of new information sharing capabilities which would provide faster electronic access to AusCheck database information.

Recommendation 22

The committee recommends that current ASIC and MSIC issuing bodies are replaced by a single, government-run, centralised issuing body.

Noted

As part of the Government's response to the Australian National Audit Office Report into the Management of the ASIC and MSIC schemes, DIT has commenced a functional review, in consultation with industry stakeholders, unions and Government agencies to identify preferred issuing body functional models and operational structures for the ASIC and MSIC schemes.

This comprehensive review will undertake a cost benefit analysis of preferred functional models, including the option of a single, government-run, centralised issuing body. It will also seek to identify potential unintended consequences – such as airport and seaport

operational issues – that may arise from the introduction of different models, as well as consider transitional issues should a new model be introduced as Government policy.