Australian Government

Attorney-General's Department

Parliamentary Joint Committee on the Australian Crime Commission

Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime

Attorney-General's Department Submission

November 2009

Introduction

The Attorney-General's Department (the Department) welcomes the opportunity to provide the Parliamentary Joint Committee on the Australian Crime Commission (ACC) with this submission as part of the Committee's inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime.

2. The Department's submission is primarily directed at paragraph (c) of the Committee's Terms of Reference:

> (c) the effectiveness of the Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) Schemes; including the process of issuing ASICs and MSICs, the monitoring of cards issued and the storage of, and sharing of, ASIC and MSIC information between appropriate law enforcement agencies.

3. The Department notes that the Australian Crime Commission (ACC), CrimTrac, the Australian Federal Police (AFP) and the Australian Customs and Border Protection Service (Customs and Border Protection) have made separate submissions to the Committee on this inquiry.

4. This submission is divided into six parts. Part 1 outlines the roles of the agencies within the Attorney-General's portfolio that are involved in aviation and maritime security and how these relate to the Terms of Reference. Part 2 provides a description of the ASIC and MSIC framework and the work of the AusCheck branch of the Department within that framework. Part 3 provides statistical information on the ASIC and MSIC schemes, including volumes, timeframes and key performance indicators, how many ASICs and MSICs have been issued, and how many applicants have been assessed as not eligible. Part 4 provides information on AusCheck's procedures for storing and sharing ASIC and MSIC scheme information. Part 5 identifies some significant issues relevant to future arrangements for background checking.

5. In preparing this submission, AusCheck has consulted with and received input from its portfolio agencies, including the AFP, the ACC, Customs and Border Protection, CrimTrac and the Australian Security Intelligence Organisation (ASIO).

Part 1: Attorney-General's portfolio – respective roles in aviation and maritime security

The Attorney-General's Department

6. AusCheck, a branch within the National Security Law and Policy Division of the Department, is currently responsible for undertaking background checking services for the issuing of ASICs and MSICs. AusCheck's role in the ASIC and MSIC schemes is primarily operational, with policy responsibility for these schemes falling within the portfolio of the Minister for Infrastructure, Transport, Regional Development and Local Government.

7. The Criminal Justice Division (CrJD) within the Department is responsible for the development of law and policy relating to organised crime. CrJD can provide information on organised crime policy and legislation.

The Australian Federal Police

8. The AFP has a broad aviation security role which includes investigation of serious and organised crime. The AFP operates the Unified Policing Model (UPM) which prescribes airport policing arrangements between the Commonwealth and the States and Territories. The UPM operates at the 11 major airports in Australia.

9. The AFP's unified policing presence comprises: Airport Police Commanders, Police Aviation Liaison Officers, Joint Airport Intelligence Groups (JAIG), Joint Airport Investigation Teams (JAIT), a Counter-Terrorist First Response (CTFR) capability and Airport Uniform Police (which include seconded State and Territory Police to the AFP). Regional Rapid Deployment Teams (RRDT's) operating from within the CTFR capability also delivers the CTFR function at regional Australian airports.

10. The JAIG provide intelligence products which inform tactical and operational decision making, while JAIT proactively target serious and organised criminality and trusted insiders who aim to exploit their positions of trust at the eleven Major Australian Airports. The JAIG and JAIT are made up of sworn AFP officers and seconded State/Territory and Australian Customs and Border Protection Service officers, with other Commonwealth officers seconded as necessary.

11. In the maritime sector the AFP is involved in a wide variety of operational activity including intelligence projects and investigations in environmental crime, people smuggling, importation/exportation of illicit goods including narcotics for example. In the port environment, the AFP is predominately operationally involved when a port is being used to facilitate importing/exporting illicit goods and in the national security regime. The AFP is directly involved in projects addressing specific areas of the maritime sector by contributing to: Strategic Maritime Management Committee work; Joint Agency Maritime Advisory Group forums including the JAMAG Information Sharing Working Group; and the Customs and Border Protection Command risk processes. The AFP is also involved in various industry and government policy meetings and working groups.

12. The AFP is continuing to work with the ACC, Customs and Border Protection, State/Territory Police and international law enforcement partners to develop and share information and intelligence on crimes impacting on the security of Australian ports and in the maritime operating environment.

13. For the AFP, border security involves a layered approach with some of the most effective strategies involving off-shore engagement with partner agencies. The AFP aims to prevent serious and organised crime groups from being able to bring illicit commodities to our shores. Engagement strategies include intelligence exchange, joint investigations, training and capacity building. This off-shore strategy assists in reducing the organised crime impact on the aviation and maritime security measures allowing an increased focus of available resources on those threats that do manifest themselves at the border.

The Australian Customs and Border Protection Service

14. As the primary inspector of air and sea cargo, Customs and Border Protection is integral to Australia's aviation and maritime security measures. Customs and Border Protection deploys its resources based on risk, using advanced screening and border clearance processing of passengers, crew, vessels and aircraft arriving and departing Australia. All high risk consignments identified are physically examined and high risk ships are boarded at their first Australian port of call.

15. Customs and Border Protection has CCTV coverage in 63 seaports and eight international airports, using over 2,000 CCTV cameras. The CCTV network is used to detect unlawful activity, provide information to inform risk assessment and collect evidentiary material.

16. Air Border Security teams provide a visible Customs and Border Protection presence in the airside aviation environment conducting border control activities and providing an intelligence collection capability.

17. Customs and Border Protection carries out random day and night patrols of ports on foot and by car, and on water to provide a visible presence, deter illegal activity and gather information and intelligence.

The Australian Crime Commission

18. The ACC is a dynamic and flexible organisation that collects and disseminates criminal intelligence and undertakes criminal investigations with its partners. This is reflected in the *Australian Crime Commission Act 2002* where the ACC's primary objective is "to collect, correlate, analyse and disseminate criminal information and intelligence and to maintain a national database of that information and intelligence". ACC work priorities are set by the ACC Board.

19. From November 2005 to June 2008, the Board authorised the Crime in the Transport Sector Determination to examine organised criminal activity in air and maritime ports. From November 2006 to December 2008 the Board also authorised the Illegal Maritime Importation and Movement Methodologies Determination, which focused on developing a broad understanding of crime within the small craft and domestic fishing environments.

20. In February 2009, the ACC released a report (*Organised Crime in Australia)* which provides a current picture of organised crime in Australia, including the key issues influencing change and the extent and impact of organised crime. This report also describes the efforts being made by law enforcement agencies in disrupting and dismantling organised crime groups.
http://www.crimecommission.gov.au/publications/oca/index.htm

21. The ACC's role is particularly relevant to paragraphs (a), (b), (c), (d) and (e) of the Terms of Reference.

CrimTrac

22. CrimTrac provides AusCheck with criminal histories necessary to perform background checks for the ASIC and MSIC schemes. CrimTrac provides this information in accordance with a Memorandum of Understanding (MoU) between the two parties.

Australian Security Intelligence Organisation

23. ASIO is responsible for gathering information and collecting intelligence that will enable it to warn the Government about activities or situations that might endanger Australia's national security. ASIO does not investigate criminal activity. With regard to the ASIC and MSIC schemes, ASIO conducts security assessments for all applicants. ASIO assesses an individual's background and any past activities to determine whether these indicate they could be a threat to national security. In providing assessments, ASIO is governed by Part 4 of the *Australian Security Intelligence Organisation Act 1979*.

Part 2: ASIC and MSIC Frameworks – AusCheck's Role

Overview

24. The ASIC and MSIC schemes are established in the *Aviation Transport Security Regulations 2005* (Aviation Regulations) and *Maritime Transport and Offshore Facilities Regulation 2003* (Maritime Regulations), and are administered by the Department of Infrastructure, Transport, Regional Development and Local Government (Infrastructure).

25. The schemes require all persons needing unescorted access to aviation or maritime security zones to display an ASIC (regulation 3.03) or MSIC (regulation 6.07J). ASICs and MSICs are not access cards and they do not provide the right of entry to a facility within an aviation or maritime security zone. Workers who may require an ASIC or MSIC include most employees based at airports, port and offshore oil and gas facilities as well as maintenance and transport workers servicing these facilities. There are approximately 120,000 current ASIC holders and 90,000 current MSIC holders.

26. In order to obtain an ASIC or MSIC, a person with an operational need to access an aviation or maritime security zone must apply in writing through an Issuing Body - which is an industry association or private company that has been authorised by the Department of Infrastructure to issue ASICs or MSICs. As part of the application process, individuals must provide the following information:

- proof of identity documents
- confirmation of right to work in Australia, and
- evidence of operational need to have an ASIC or MSIC.

See regulation 6 of the *AusCheck Regulations 2007* at Attachment A.

27. All individuals who apply for an ASIC or MSIC (with the exception of people under the age of 18) must be background checked to determine eligibility. The elements of the background checking arrangements that underpin both the ASIC and MSIC schemes are as follows:

- a criminal record check by AusCheck
- a security assessment by ASIO, and
- if required, a right to work check by the Department of Immigration and Citizenship (DIAC).

See section 5 of the *AusCheck Act 2007* at Attachment B.

28. The eligibility criteria (offences which disqualify a person from holding an ASIC or MSIC) are set out in regulation 6.01 of the Aviation Regulations and regulation 6.07C of the Maritime Regulations. See Attachment C.

Background checking by AusCheck

29. AusCheck's role is to perform relevant background checks to determine if a person is eligible to hold an ASIC or MSIC.

30. AusCheck commences background checking once it receives the relevant information from an Issuing Body (see paragraph 23). Once this information is received, it is automatically forwarded by AusCheck's IT system to ASIO for a security assessment and to CrimTrac for a National Criminal History Record Check (NCHRC).

31. If an individual has no criminal history, the process is completely automated. CrimTrac will notify AusCheck electronically, and AusCheck will then notify the applicant's Issuing Body that the applicant is eligible for an ASIC or MSIC. This process can be completed within a day.

32. If an NCHRC check 'matches' an individual to a criminal history, the criminal history certificate (i.e. criminal record) is sent electronically (subject to relevant spent convictions/non-disclosure legislation) to AusCheck. AusCheck then assesses whether an individual is eligible for an ASIC or MSIC, based on the relevant criteria set out in the Aviation Regulations and Maritime Regulations.

33. AusCheck will find that a individual is either:

- eligible for an ASIC or MSIC
- not eligible for an ASIC or MSIC, or
- 'eligible with conditions'(this applies to the ASIC scheme only and will result in the card having a validity period of 12 months instead of two years)

34. If an individual is assessed as not eligible, AusCheck will issue a directive to the individual's Issuing Body not to issue a card.

35. Before finalising an 'adverse' decision (i.e. a finding of not eligible or eligible with conditions), AusCheck is required to write to the individual and notify them of a

possible adverse decision. The individual is given a minimum of 28 days to provide further information of relevance to their eligibility for an MSIC or ASIC – eg that there are errors on their criminal history.

36. If AusCheck makes an adverse final finding, both the individual and Issuing Body are notified. The Secretary of the Department of Infrastructure may also be notified in certain cases. The individual is entitled to appeal a decision to the Administrative Appeals Tribunal (AAT), or apply for a discretionary ASIC or MSIC from the Department of Infrastructure based on mitigating factors, such as how long ago the offence was committed and the circumstances surrounding the offence.

37. Issuing Bodies must maintain a register of all MSICs or ASICs it has issued, including cards that have expired or been cancelled.

Part 3: Statistics Relating to AusCheck's Performance and Findings of Eligibility

AusCheck Key Performance Indicators

38. In the 12 months from 1 October 2008 to 30 September 2009, AusCheck undertook 75,415 background checks for the ASIC and MSIC schemes (56,971 for ASICs and 18,444 for MSICs).

39. AusCheck performance is measured against a set of Key Performance Indicators – which is for AusCheck's part in the background checking process to be completed in five (5) business days or less 98 per cent of the time (i.e. excluding time awaiting responses from checking partners or the person being checked).

40. The following table reports the completion rates of background checking for the third quarter (June, July, August) of 2009. During the third quarter, AusCheck performed 90% of its part on the checking process on the same day. Within five days, this figure increases to 99.30%. Applications which take greater than five days to complete are usually the result of the applicant having an adverse criminal history. In such a case, the individual is allowed a minimum of 28 days to furnish AusCheck with information before AusCheck makes a final decision on the application.

	All Checks	AusCheck
Same Day	0%	90%
5 days	68%	99.30%
10 days	80%	99.40%
15 days	89%	99.50%
20 days	96%	99.60%
20 days +	4%	0.30%

The 'All Checks' column reports on the completion rates of applications for ASICs and MSICs completed and returned to issuing bodies within the corresponding timeframe.

The 'AusCheck' column reports on AusCheck's timeframe(s) to complete its part of the checking process during the reporting period, i.e. excluding those awaiting completion of CrimTrac and ASIO checks.

AusCheck Statistics for MSIC and ASIC Applications

ASIC

41. From 1 October 2008 to 30 September 2009, AusCheck completed 56,971 ASIC applications, with 215 applicants (0.37%) determined to be ineligible to hold an ASIC. The most common reasons why these applicants were found ineligible include offences relating to dishonesty (60.46%) which includes theft, embezzlement and fraud; and violence (29.30%), which includes offences such as assault and kidnapping.

ASIC - Applications	Number of applications July 09 to Sept 09	Total Number of applications from Oct 08 to Sept 09
Number of ASIC applications completed	18 844	**56,971**
Of those completed number of applications with disclosable criminal offences	1 441 (7.65%)	**4,956** (8.69%)
Of those completed number with a finding of Not Eligible	51 (0.27%)	**215** (0.37%)
Reasons for Not Eligible		
- Drug Offences	4	**19**
- Violence	13	**63**
- Dishonesty	34	**130**
- Damage to Property	0	**3**
Of those completed number with a finding of Eligible with Conditions ie 12 month validity only	88 (0.47%)	**371** (0.65%)

MSIC

42. From 1 October 2008 to 30 September 2009, AusCheck completed 18,444 MSIC applications, with 69 applicants (0.37%) determined to be ineligible to hold an MSIC. The most common reason why these applicants were found ineligible was drug-related offences (95.65%).

MSIC - Applications	Number of applications July 09 Year to Sept 09	Total Number of applications from Oct 08 to Sept 09
Number of MSIC applications completed	4 392	**18,444**
Of those completed number of applications with disclosable criminal offences	920 (20.95%)	**3884** (21.05%)
Of those completed number with a finding of Not Eligible	21 (0.47%)	**69** (0.37%)
Reasons for Not Eligible		
- Drug Offences	20	**66**
- False Identity or False Documents Offences	0	**1**
- Organised Crime/Money Laundering	1	**2**

Part 4: Storage and Sharing of Information on the AusCheck Database

Retention of Information by AusCheck

43. Under the *AusCheck Act 2007* (AusCheck Act), AusCheck is authorised to establish and maintain a database that contains information pertaining to ASIC and MSIC holders. Information that AusCheck retains includes the cardholder's name, residential address, date of birth, card number and the date the card was issued.

44. Under an MoU with CrimTrac, AusCheck must destroy Criminal History Information (CHI) within 3 months of receipt, unless the particular information is subject to review or appeal to the AAT. Other information, such as personal details, is retained under the *Archives Act 1983* and the Department's records disposal arrangements.

45. The *AusCheck Amendment Act 2009*, currently before Federal Parliament, will specify that AusCheck must not retain any identity verification information. AusCheck will only be authorised to pass this information to law enforcement agencies, or return it to the individual.

Sharing of Information

46. Section 14(2) of the AusCheck Act specifies that personal information held in the AusCheck database may be used or disclosed for:

> The collection, correlation, analysis or dissemination of criminal intelligence or security intelligence by the Commonwealth, or by a Commonwealth authority that has functions relating to law enforcement or national security, for purposes relating to law enforcement or national security.

47. The following agencies are currently recognised by AusCheck as having functions relating to law enforcement or national security for the purposes of the AusCheck Act:

- the AFP
- Customs and Border Protection
- The ACC, and
- ASIO.

48. Since September 2007, AusCheck has received and granted 32 requests for information from its database. These requests were made by the AFP, the ACC and Customs and Border Protection.

49. To give greater certainty regarding the disclosure of information to Commonwealth law enforcement and intelligence agencies, the Secretary of the Attorney-General's Department has issued *Guidelines for Accessing Information on the AusCheck Database*. These are also available on the Department's website. The Guidelines establish a compulsory framework for decision making by AusCheck staff in determining the legality of requests for personal information from the database.

http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_BackgroundChecking_GuidelinesforAccesstotheAusCheckDatabase.

50. In accordance with these Guidelines, only certain persons within law enforcement and intelligence agencies can request access to AusCheck's database. Prior to AusCheck disclosing the requested information, the requesting agency must provide AusCheck with a written undertaking that the supplied information will only be accessed and used for purposes relating to law enforcement or national security. Once the requesting agency has received the information from AusCheck's database, they are required to ensure that the information is dealt with in a way that complies with all relevant privacy, record-keeping, records disposal, auditing and reporting requirements.

Privacy Controls

51. AusCheck applies strict privacy controls to all of its areas of operation. AusCheck was a finalist in the Australian Privacy Commissioner's 2008 Privacy Awards[1]. The awards recognise and reward businesses and government agencies that engage in good privacy practices.

52. To further enhance privacy controls in the AusCheck Scheme, the AusCheck Amendment Bill 2009 will insert a new offence relating to disclosure of personal information by third parties. Under the provision, an individual will commit an offence if that person has obtained AusCheck information and disclosed that information to someone else in circumstances not authorised by the AusCheck Act. For example, a law enforcement agency that has been lawfully disclosed AusCheck information will commit an offence if that information is forwarded to a third party without authorisation from AusCheck.

Memoranda of Understanding with Agencies

53. AusCheck has MoUs in place with its primary checking partners CrimTrac and ASIO as well as the Office of Transport Security within the Department of Infrastructure. These MoUs address a number of issues including any relevant financial arrangements between the parties but the principal concern is the exchange of information. AusCheck's MoUs also contain provisions to ensure that the personal information delivered to checking partners and the information provided by them are communicated and stored in a manner consistent with privacy protection principles.

[1] Media release on privacy award: http://www.privacy.gov.au/materials/types/media/view/6232. See also AGD Annual Report 2008-2009: http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_AnnualReports_AnnualReport2008_AnnualReport2008-09

Part 5: Future considerations for effective background checking

54. The ASIC and MSIC schemes are key components of the Commonwealth's efforts to minimise the threat of terrorism and unlawful interference in Australia's maritime transport and offshore facilities, and the aviation transport sector. The ASIC and MSIC schemes were established to help reduce the risk of terrorism and unlawful interference to maritime and aviation transport respectively

55. The MSIC scheme was the first of its kind in the world to check the background of all persons who have unmonitored access to sensitive areas of ports, port facilities, ships and offshore facilities. To date, only Australia, the United States and Canada have implemented national background checking processes in the maritime sector.

56. The current ASIC and MSIC arrangements have many strengths, however, enhancements to current background checking arrangements can be made in the future. It must be noted that any enhancements will have some impact on individuals, industry and Government agencies.

Continuous Checking

Nature of Issue

57. As noted above, AusCheck conducts criminal history checks through CrimTrac's National Police Checking Service. Each criminal history check applicant's information is run against CrimTrac's National Names Index (NNI). The NNI database holds the names of persons of interest to Australia's police services. If a hit against NNI occurs, a referral is created which is sent to the relevant Australian police service who then provide point-in-time CHI. This CHI is then sent to AusCheck to form part of an ASIC or MSIC background check.

58. There is currently no mechanism for CrimTrac to send 'updated' CHI to AusCheck (or its other checking partners) – for example, to determine if an individual has been convicted of a new offence – between background checks. It was suggested by the Wheeler Review[2] that information held by police forces in Australia should also be made continuously available to the central authorising agency responsible for background checking.

59. The ASIC scheme requires card holders to inform their Issuing Body within seven days if they are convicted of an offence which affects their eligibility to hold an ASIC. If an individual is also sentenced to imprisonment, the Issuing Body must immediately cancel the ASIC and inform AusCheck within 48 hours. If an individual fails to tell their Issuing Body that they have been convicted of a relevant offence, the offence is unlikely to be discovered until the individual renews their ASIC. See regulations 6.41 and 6.43 of the Aviation Regulations and regulation 14 of the AusCheck Regulations 2007. There is currently no obligation for an MSIC holder to report maritime-security-relevant-offences to their Issuing Body (or AusCheck).

[2] Paragraph 55, the Wheeler Review.

Possible Options

60. CrimTrac is investigating the feasibility of supplying continuous updates on selected criminal records. This would help to reduce the system's current reliance on individual card holders self-reporting.

Considerations

61. The ability of CrimTrac to supply real-time, continuous criminal history information would require high-levels of connectivity between police, law enforcement agencies and stakeholders. This is a significant task under active consideration that will require the joint efforts of relevant State, Territory and Commonwealth agencies and would take time to implement.

Name-based Checks and Biometric Checks

Nature of Issue

62. NCHRC's are name-based checks. Individuals are required to submit details of their full name and birthdates, which is compared against information on CrimTrac's central database. Criminal history is then released to AusCheck, subject to relevant spent convictions and non-disclosure legislation.

63. Name based checks are not based on 'unique identifiers' (i.e. an object or thing that can be definitively linked to an individual – such as a fingerprint). Difficulties arise in name-based checks where individuals have similar names and birthdates.

Possible Options

64. An alternative to a name-based check is a check based on a unique biometric identifier in combination with a person's name. The Wheeler Review[3] into aviation security recommended the introduction of biometrics such as fingerprints or facial recognition technology as part of the aviation security framework in Australia.

65. The use of a fingerprint check could streamline background checking processes by ensuring accuracy in identifying individuals. For example, it takes longer to perform criminal history checks on individuals with common names because they are more likely to return several criminal histories. CrimTrac must manually sort through all of these criminal histories to ensure the correct criminal history is matched with the correct applicant.

66. The National Automated Fingerprint Identity System (NAFIS) administered by CrimTrac matches fingerprints collected from an individual against the fingerprints of criminal offenders. Fingerprints are currently used by the casino and gaming industries for background checking and identification purposes.

[3] Page 73, the Independent Review into Airport Security and Policing in Australia (the Wheeler Review) 2005.

Considerations

67. While fingerprinting is much more reliable than in the past because of the use of digital technology, concerns remain about storage, use and collection of biometric information. This was evident in the Senate Legal and Constitutional Legislation Affairs Committee Report into the AusCheck Amendment Bill 2009, which acknowledged that the use of biometric data was not to be entered into lightly, or without rigorous examination. The Report also recommended that AusCheck not be permitted to deal directly with biometric data except to pass it onto appropriate agencies (such as CrimTrac). As a result, the amendments in the Bill will make it clear that AusCheck cannot collect, use or store biometric information.

Current Way Forward

68. As the use of biometrics can provide a means in the future to better anchor an individual's identity, AusCheck will closely monitor developments in this area, including exploring the prospect of cooperating with agencies such as CrimTrac, as a possible means of streamlining background checking.

Provision of Information to Law Enforcement in Real Time

Nature of Issue

69. Consistent with the recommendations of the Senate Legal and Constitutional Legislation Affairs Committee Report into the *AusCheck Act 2007*, AusCheck is currently restricted from providing law enforcement and intelligence agencies, such as the AFP and ASIO, with real-time access to information stored on AusCheck's database. Under the current Guidelines, agencies are provided with information from the AusCheck database which has been copied onto a CD or in a written document, and hand delivered. This restricts the ability of law enforcement agencies to use AusCheck database information in operationally critical circumstances.

Options

70. AusCheck is exploring the feasibility of establishing an MoU with the AFP to provide information from the AusCheck database in real time, for law enforcement or national security purposes. This MoU will not give the AFP physical access to the database (AusCheck would still be required to download the information from the database), and will ensure that access is consistent with the procedural requirements of the Guidelines, the AusCheck Act and AusCheck Regulations.

Considerations

71. In negotiating the MoU, AusCheck is cognisant of the Senate Committee on Legal and Constitutional Affairs recommendations regarding the disclosure of information contained in the AusCheck database.

Way forward

72. AusCheck will consider if it is appropriate to enter into similar agreements with other law enforcement and intelligence agencies, such as Customs and Border Protection, on a case-by-case basis.

Access to Database by States and Territories

Nature of Issue

73. Currently, access to the database is restricted under the AusCheck Act to *Commonwealth* authorities. This precludes States and Territories from obtaining information on AusCheck's database even if they have legitimate law enforcement or national security reasons for accessing the information.

Options

74. In order to provide for the legitimate requirements of State and Territory law enforcement authorities, the AusCheck Act could be amended to extend access to the AusCheck database to State and Territory authorities that have functions relating to law enforcement or national security, for purposes relating to law enforcement or national security.

Considerations

75. The Senate Legal and Constitutional Legislation Affairs Committee Report into the *AusCheck Act 2007* recommended that strict provisions be placed on the sharing of AusCheck's database information with law enforcement agencies.

Attachment A

AusCheck Regulations 2007

6 Information to be included in application

(1) An application for a background check must include the following information about the individual to whom the background check relates:

(a) the individual's name, gender and date and place of birth;

(b) the individual's residential address;

(c) the name and business address of the individual's employer;

(d) the individual's contact details;

(e) for a background check that relates to whether the individual is an unlawful non-citizen or holds a visa entitling him or her to work in Australia:

(i) the number and country of issue of any passport issued to the individual; and

(ii) the number and expiry date of any visa granted to the individual enabling the individual to travel to and enter, or remain in, Australia.

(2) For paragraph (1) (d), an individual's ***contact details*** are:

(a) the individual's preferred mailing address; and

(b) the individual's preferred telephone contact number (which may be a home, business or mobile number); and

(c) the individual's email address, if the individual chooses to give it.

Attachment B

AusCheck Act 2007

5 Definition of *background check*

A ***background check***, in relation to an individual, is an assessment of information relating to one or more of the following:

(a) the individual's criminal history;

(b) matters relevant to a security assessment of the individual;

(c) the individual's citizenship status, residency status or the individual's entitlement to work in Australia, including but not limited to, whether the person is an Australian citizen, a permanent resident or an unlawful non-citizen;

(d) verification checks of documents relating to the identity of the individual.

Attachment C

Maritime Security Relevant Offences

For the purposes of the *Maritime Transport and Offshore Facilities Security Regulations 2003*, a Maritime security relevant offence is an offence of a kind mentioned in the following table against a law of the Commonwealth, or of a State or Territory, or of any other country or part of country:

1.	An offence mentioned in Chapter 5 of the Criminal Code. Note Offences for this item include treason, espionage and harming Australians.
2.	An offence involving the supply of goods (such as weapons or missiles) for a Weapons of Mass Destruction program as mentioned in the *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995*
3.	An offence involving the hijacking or destruction of an aircraft or vessel
4.	An offence involving treachery, sabotage, sedition, inciting mutiny, unlawful drilling, or destroying or damaging Commonwealth property, mentioned in Part II of the *Crimes Act 1914*
5.	An offence involving interference with aviation, maritime transport infrastructure or an offshore facility, including carriage of dangerous goods on board an aircraft or ship, or endangering the security of an aerodrome, a port or an offshore facility
6.	An identity offence involving counterfeiting or falsification of identity documents, or assuming another individual's identity
7.	Transnational crime involving money laundering, or another crime associated with organised crime or racketeering
8.	People smuggling and related offences mentioned in Chapter 4, Division 73 of the *Criminal Code*
9.	An offence involving the importing, exporting, supply or production of weapons, explosives or a trafficable quantity of drugs.

Aviation Security Relevant Offences

For the purposes of the *Aviation Transport Security Regulations 2005*, an aviation security relevant offence is an offence of a kind mentioned in the following table against a law of the Commonwealth, or of a State or Territory, or of any other country or part of country:

1. An offence involving dishonesty
2. An offence involving violence or a threat of violence
3. An offence involving intentional damage to property or a threat of damage to property
4. An offence constituted by the production, possession, supply, import or export of a substance that is: (a) a narcotic substance within the meaning of the *Customs Act 1901*; or (b) a drug within the meaning of: i. regulation 10 of the *Customs (Prohibited Exports) Regulations 1958*; or ii. regulation 5 of the *Customs (Prohibited Imports) Regulations 1956*
5. An offence, of a kind dealt with in Part 11 of the *Crimes Act 1914* against the Government of the Commonwealth or a State or Territory or a country or part of a country other than Australia
6. An offence against Part 2 of the *Crimes (Aviation) Act 1991*
7. An offence against Part 5.3 of the *Criminal Code*
8. An offence constituted by the production, possession, supply, import or export of explosives or explosive devices