The Auditor-General
Audit Report No.39 2010–11
Performance Audit

Management of the Aviation and Maritime Security Identification Card Schemes

Attorney-General's Department

Department of Infrastructure and Transport

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81185 7

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
webmaster@anao.gov.au

Australian National Audit Office

Canberra ACT
5 May 2011

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Attorney-General's Department and the Department of Infrastructure and Transport in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to *Senate Standing Order 166* relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Management of the Aviation and Maritime Security Identification Card Schemes*

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team
Charles Higgins
Edwin Apoderado
Tom Clarke

Contents

Tables

Figures

Abbreviations

AGD	Attorney-General's Department
ANAO	Australian National Audit Office
ASIC and MSIC schemes	Aviation and Maritime Security Identification Card schemes
ASIO	Australian Security Intelligence Organisation
ATS Act	*Aviation Transport Security Act 2004*
ATS Regulations	Aviation Transport Security Regulations 2005
AusCheck Act	*AusCheck Act 2007*
DIAC	Department of Immigration and Citizenship
DIT	Department of Infrastructure and Transport
MTOFS Act	*Maritime Transport and Offshore Facilities Security Act 2003*
MTOFS Regulations	Maritime Transport and Offshore Facilities Security Regulations 2003
OPAC	OTS Policy and Audit Committee
OTS	Office of Transport Security
VIC	Visitor identification card

Summary and Recommendations

Summary

Introduction

1. The Aviation and Maritime Security Identification Card schemes (ASIC and MSIC schemes) were introduced by the Australian Government to enhance the existing 'layers of security' designed to safeguard the aviation and maritime industries.[1] ASICs and MSICs are displayed by individuals to demonstrate that the holder has had their background checked and is permitted to be in the 'secure areas' of aviation and maritime zones (typically specific parts of airports, seaports and offshore facilities, such as oil and gas rigs). ASICs and MSICs are generally required by a range of people who work in secure zones, including: airline staff; airport service workers; baggage handlers; port service workers; stevedores; and transport operators such as train and truck drivers.

2. The ASIC and MSIC schemes are established by the *Aviation Transport Security Act 2004* (ATS Act) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFS Act). The aim of the schemes is to: safeguard against unlawful interference with Australia's aviation, maritime transport and offshore facilities, and to reduce the risk of terrorist infiltration.

3. The ASIC and MSIC legislation prescribes a range of conditions for the use of the cards and the eligibility criteria for obtaining an ASIC or MSIC. Table S 1 outlines the broad key criteria for obtaining an ASIC or MSIC.

[1] Australia's current approach to transport security relies on activities across the following complementary layers: intelligence to identify threats; targeted mitigation strategies at last ports of call (the point of departure) to detect and interdict risks before they depart for Australia; law enforcement measures; security measures at airports, seaports and offshore facilities, including preventive physical and identity security measures and access control; passenger, baggage and cargo screening; and aircraft, ship and offshore facilities security. Commonwealth of Australia, *Counter-Terrorism White Paper*, 2010.

Table S 1

Criteria for obtaining an ASIC and MSIC

Criteria	Description
Operational need	Aviation—a person who has a need for frequent access to a secure area relating to the operation of an airport or an aircraft; and Maritime—if occupation or business interests require or will require unmonitored access to a maritime security zone at least once a year.
Identity verified	An individual's identity is verified primarily through the production of credentials.
Criminal history	The person does not have an adverse criminal record.
Security assessment	The person is not the subject of an adverse security assessment.[2]
Citizenship/ immigration	Aviation—either an Australian citizen or the issuing body is satisfied that the person is not an unlawful non-citizen; and Maritime—either an Australian citizen or valid visa to work in Australia.

Source: Aviation Transport Security Regulations 2005 (ATS Regulations) and Maritime Transport and Offshore Facilities Security Regulations 2003 (MTOFS Regulations).

Overview of management arrangements for the ASIC and MSIC schemes

4. There is a diverse range of government and industry bodies involved in the management and delivery of the ASIC and MSIC schemes. This includes over 1200 industry participants, including airports, airlines and seaports, which are required to develop security plans that outline arrangements by which access to designated secure areas is restricted to ASIC and MSIC holders.

5. Further, more than 200 government and non-government bodies have been authorised to issue ASICs and MSICs. These issuing bodies have a range of responsibilities under the ATS and MTOFS Acts relating to the production and issue of ASICs and MSICs. For many applicants, the relevant issuing body is their employer, local airport or seaport. However, the schemes also allow commercially based 'third party' issuing bodies that do not necessarily have a direct relationship to the applicant to issue ASICs and MSICs. The cards produced by issuing bodies include a tamper-evident feature designed to reduce the risk of forgery.

[2] The definition of 'security assessment' under both the ATS Regulations and MTOFS Regulations has the same meaning as in Part IV of the *Australian Security Intelligence Organisation Act 1979*.

6. The Department of Infrastructure and Transport (DIT) administers the ATS Act and MTOFS Act on behalf of the Australian Government. Within DIT, the Office of Transport Security (OTS) has principal responsibility for administering transport security. OTS's primary role as the transport security regulator is the approval of transport security plans and monitoring compliance with approved plans. In relation to the ASIC and MSIC schemes, OTS approves ASIC programs and MSIC plans, on behalf of the Secretary, and monitors the compliance of industry participants, issuing bodies and cardholders.

7. Central to the ASIC and MSIC schemes is the requirement that applicants have their background checked. The *AusCheck Act 2007* (AusCheck Act), administered by the Attorney-General's Department (AGD), establishes the processes for the background check. AusCheck, a branch within AGD, coordinates the background check. The check involves a criminal records check coordinated by CrimTrac; a security assessment by the Australian Security Intelligence Organisation; and if relevant, a citizenship or immigration check, conducted by the Department of Immigration and Citizenship. AusCheck is also responsible for maintaining the AusCheck database, the consolidated database of all ASIC and MSIC cardholders. As at 30 June 2010 there were 265 328 valid issued cards (126 806 ASICs and 138 522 MSICs) recorded on the AusCheck database.

8. Table S 2 summarises the key responsibilities of the parties involved in the ASIC and MSIC schemes.

Table S 2

Key ASIC and MSIC responsibilities

Party	Key ASIC and MSIC Responsibility
Industry participants (airports, ports etc)	Developing security plans and ensuring that access to security zones is limited to ASIC and MSIC holders.
Issuing bodies (airports, ports, third party bodies etc)	Issuing ASICs and MSICs only to individuals who have been checked through AusCheck and meet regulatory requirements.
OTS	Approving transport security plans; and monitoring the compliance of industry participants, issuing bodies, and cardholders.
AusCheck	Coordinating background checks on ASIC and MSIC applicants and maintaining the AusCheck database.
Cardholders	Meeting eligibility criteria and displaying ASICs and MSICs in security zones.

Source: ANAO analysis.

9. Historically, there has been significant interest in the role of ASICs and MSICs in relation to their contribution to the security of the aviation and maritime industries. Parliamentary and internal reviews have highlighted a number of inherent vulnerabilities associated with having a large number of issuing bodies, as well as the return of expired or cancelled cards and visitor management. Most recently, the *National Aviation Policy White Paper: Flight Path to the Future*,[3] released in 2009, included a commitment to strengthening the ASIC scheme to address some of these identified vulnerabilities. Measures to strengthen the cancellation provisions for issuing bodies and tighten visitor management arrangements are in the process of being implemented.

Audit objectives, criteria and scope

10. The objective of the audit was to assess the effectiveness of DIT's and AGD's management of the ASIC and MSIC schemes.

11. In assessing the performance of DIT and AGD, the ANAO examined the effectiveness of the: governance arrangements supporting the schemes; process for issuing cards; information technology (IT) environment supporting the schemes; and compliance activities surrounding the schemes.

12. The scope was confined to the role undertaken by DIT and AGD; it did not examine the work of others with an interest in the ASIC and MSIC schemes, such as law enforcement and national security agencies.

Overall conclusion

13. The ASIC and MSIC schemes form part of the Australian Government's layered approach to safeguarding the aviation and maritime industries against terrorism and other unlawful acts. This approach requires judgements to be made about the appropriate balance between the risk of such acts occurring and the impact mitigation strategies, such as security cards, may have on the efficient operations of these facilities.

14. Consistent with their legislative frameworks, the ASIC and MSIC schemes provide for the involvement of a range of entities, including both industry organisations and Australian Government agencies. OTS, a division within DIT, administers the regulatory framework for the schemes on behalf of the Australian Government, and AusCheck, a branch within AGD, coordinates

[3] Commonwealth of Australia, *National Aviation Policy White Paper: Flight Path to the Future*, 2009.

the background checks of ASIC and MSIC applicants. There are also over 1200 industry participants that regulate access to secure areas where the display of ASICs and MSICs is required, in excess of 200 bodies that are authorised to issue the cards, and some 250 000 cardholders, who are required to meet their obligations to properly display a valid security card while in a secure area.

15. The successful implementation of the ASIC and MSIC schemes has meant that, with some specific exceptions,[4] all persons who legitimately enter and remain in a secure area of an airport, seaport or offshore facility must now have been assessed as meeting the criteria for an ASIC or MSIC, including having their background checked, and must display their card appropriately. The arrangements put in place by OTS and AusCheck to administer the schemes reflect legislative requirements and facilitate the timely issue of security cards. However, some of the risks associated with the current delivery model could be better managed by OTS. These risks primarily relate to issuing bodies and visitor management and are inherent in the devolved nature of the schemes.

16. As previously noted, the regulatory framework of the ASIC and MSIC schemes includes over 200 authorised issuing bodies that process applications, produce and issue the identification cards. The majority of cards (80 per cent), however, are issued by a small number (20 per cent) of issuing bodies. Further, 35 per cent of all cards are issued by commercially based 'third party' issuing bodies, that have a limited ongoing relationship to the applicant. While the schemes prescribe mandatory standards for issuing bodies, these standards are not being consistently met by some issuing bodies. This includes how an applicant's operational need for the card is established and maintaining adequate records to demonstrate that an applicant's identity has been confirmed.

17. OTS has developed a compliance framework that aims to cooperatively encourage compliance through education and audit activities, with the focus being on high-risk participants. While the framework is appropriately targeted at high-risk participants, it could be strengthened if information obtained

[4] This includes passengers who are boarding or disembarking from an aircraft; supervised visitors to secure areas, crew of a foreign aircraft, crew members of certain ships and emergency personnel who are responding to an emergency.

through OTS's audit, inspection and stakeholder programs was used to better inform and focus the schemes' compliance activities.

18. A further area of concern is visitors entering secure areas at airports. Visitors can obtain a visitor identification card (VIC)[5] and, although a VIC holder must be supervised, they do not need to undergo the background check required for an ASIC. Concerns about the VIC regime have been raised by the Joint Committee of Public Accounts and Audit over a number of years. Revised regulations to tighten the VIC scheme are being developed, although these changes have been slow to eventuate. The total number of VICs being issued is not known, but around 40 000 were issued at one delivery gate alone at a major airport in 2009–10. Moreover, many VICs are issued repeatedly to the same individuals, effectively bypassing the ASIC background checking process. Better information on the actual usage of VICs would also assist OTS to manage this potential risk to the ASIC scheme.

19. It is difficult to obtain a reliable count of the total number of current ASIC and MSIC cards, or the currency of all cards on the AusCheck database. This is despite the database being established to provide a comprehensive record of all ASIC and MSIC applicants and cardholders. Each issuing body also maintains a database of its cardholders. Although AusCheck has developed a range of controls over the integrity of the information entered into its database, changes in one database do not always flow through to the other. As a consequence the two data sets differ markedly. More focused compliance activity would give AusCheck and OTS greater assurance around the procedures and practices adopted by issuing bodies as well as the accuracy of their databases.

20. OTS has been working with industry stakeholders on a range of strategies to manage some of the vulnerabilities identified by this audit and previous reviews. These include implementing changes to the frequency of background checks, cancellation provisions for ASIC issuing bodies, and the tightening of eligibility rules for VICs. As these changes are still to be bedded down, their capacity to mitigate these risks to the schemes' effectiveness is yet to be demonstrated. While recognising that a balance needs to be struck between the impact of regulation on industry and the achievement of the

[5] The Aviation Transport Security Regulations 2005 prescribe rules for the display and issuing of VICs for supervised visitors within aviation secure areas. There is no equivalent card for maritime and offshore facilities.

Government's security objectives for the ASIC and MSIC schemes, continued management focus on these identified vulnerabilities is warranted. To this end, the ANAO has made three recommendations aimed at further improving the effectiveness of these areas and the overall management of the ASIC and MSIC schemes.

Key findings

Governance arrangements

21. There has been an ongoing evolution in the broad structures of governance put in place by OTS and AusCheck to support the implementation of the ASIC and MSIC schemes. OTS has implemented an organisational structure that allows it to implement, monitor and coordinate tasks and deliverables. It has also developed an appropriate framework for monitoring and reporting activities. Key operational risks were documented and updated in OTS's risk register, and had clear mitigation strategies. In addition, the activities of AusCheck are subject to the Government's cost recovery policy and it has established effective processes to identify the price structure and cost of its regulatory activities over the course of the program's life.

22. The *National Aviation Policy White Paper: Flight Path to the Future* (White Paper),[6] released in 2009 included a commitment to strengthening the ASIC scheme to address some previously identified vulnerabilities. OTS, in responding to the White Paper, has developed and is currently implementing proposed changes to the ASIC scheme. These changes, which include strengthening the cancellation provisions for ASIC issuing bodies and tightening the provisions for visitor management will not, however, directly address all the identified vulnerabilities. For example, while there is a proposal to reduce the number of issuing bodies, the proposal will remove inactive issuing bodies and provide a transitional pathway for other issuing bodies to cease operations. It will not address the inconsistencies in the approaches taken by many bodies currently issuing the cards and that are not meeting the required standards.

[6] Commonwealth of Australia, *National Aviation Policy White Paper: Flight Path to the Future*, 2009.

The process for issuing ASICs and MSICs

23. The application process for ASICs and MSICs involves a wide range of stakeholders and different processes. The schemes rely on each participant understanding, and correctly applying, the legislative process. As previously mentioned, more than 200 government and non-government bodies have been authorised to issue ASICs and MSICs. These issuing bodies includes airlines, airports and seaports as well as commercially based 'third party' issuing bodies that do not necessarily have a direct relationship to the applicant. The role of OTS in these circumstances is to provide guidance and assistance, and to gain assurance from each issuing body that they are fulfilling their obligations to the required standard.

24. There are a range of practices in the issuing of ASICs and MSICs that reduce the assurance that the schemes' requirements are being met to appropriate standards. These include:

- third-party issuing bodies complying with mandatory standards in how an applicant's operational need for the card is established; and
- the evidence to demonstrate confirmation of an applicant's identity. Records maintained by issuing bodies to confirm the identity of the applicant were incomplete. For two issuing bodies assessed by the ANAO the required identity credentials were not available for 33 per cent of the applications reviewed.

25. ASICs and MSICs are made using specialised stamping machines and licensed technology. There are 25 entities that have the machines to make the cards—24 of which are also issuing bodies under the ASIC and MSIC schemes. Consequently, many issuing bodies do not produce the cards themselves, instead they use other entities to produce the cards on their behalf. Some 37 per cent of all ASICs and MSICs are made by an entity other than the issuing body. Presently, OTS has a relationship with the company that makes the stamping machines, and with most entities that use the machines to make the cards, by virtue of them also being issuing bodies under the ASIC and MSIC schemes. However, one card maker that has produced some 35 000 cards, is not an issuing body, and is therefore not subject to any formal ongoing oversight by OTS.

26. AusCheck also plays a central role in the process for issuing ASICs and MSICs by providing background checks for issuing bodies. This role includes assessing each applicant's details against the legislative criteria and making a

final recommendation whether these criteria have been met by the applicant. The ANAO's analysis of a sample of 88 applicants indicated that AusCheck assessors correctly assessed the criminal history against the legislative requirements for all the applications reviewed. The ANAO also analysed 20 recent applicants with conditional or adverse assessments. AusCheck had complied with the legislative requirements, including procedural fairness and notification of appeal rights, for these applications. It has also developed standard operating procedures, checklists and templates to support its decision–making processes.

27. ASIC and MSIC applications are processed in a timely manner. Based on an extract of the AusCheck database in June 2010, AusCheck processed 97 per cent of its background checking activity within one day and 99 per cent was completed in five business days or less. In terms of the 'end-to-end' processing time, around 50 per cent of checks were completed within two weeks. The total time of a background check may also be affected by the time an application is assessed by background checking partners.

28. Rejected applicants can apply for a discretionary ASIC or MSIC and provide additional information that demonstrates that the person is unlikely to be a threat to aviation or maritime security—this occurred 112 times in 2009–10. OTS has developed a range of templates, checklists and 'how to guides' to support the processing of the discretionary cards. The ANAO reviewed 21 applications and these were generally processed in accordance with legislative requirements. OTS applied a risk-based, evidence-informed approach in assessing whether the applicant represented a risk to transport security.

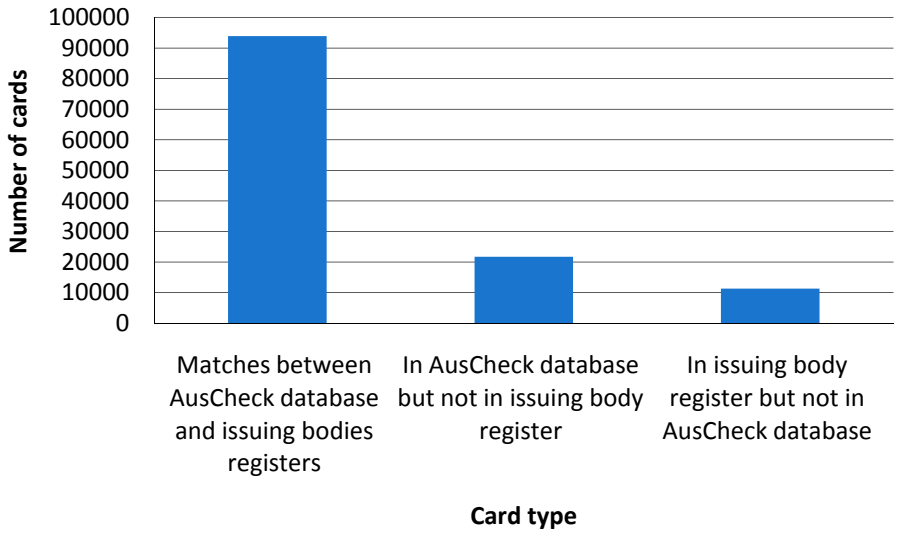
Information management

29. AusCheck, in processing and maintaining a central register of all ASICs and MSICs, relies on one main information technology system. An inherent risk with the AusCheck database is that there is no direct and ongoing link between this database and the issuing bodies' data holdings. To mitigate this risk, AusCheck has implemented mandatory controls over the input of data, including data field validation, and access is controlled through formalised processes.

30. The AusCheck database was established to provide a 'comprehensive database of all applicants and ASIC and MSIC cardholders.'[7] Each issuing body also maintains a database of its cardholders. Comparison of AusCheck data with issuing body data for 50 per cent of all cardholders by the ANAO identified significant variances. For example, there was a significant number of cards registered on the AusCheck database that were not in an issuing body's register. There were also cards registered in issuing bodies' registers but not in the AusCheck database. Figure S 1 provides a summary of the total figures within each population.

Figure S 1

Number of cards from selected issuing bodies matched against the AusCheck database



Source: ANAO analysis of AusCheck and issuing body data.

31. These variances were largely due to administrative or process differences and errors. While the differences between the databases can be partly explained by the devolved nature of the ASIC and MSIC schemes, they do reduce confidence in the accuracy of the total number of current cards, and the currency of the data in the AusCheck database. Currently, OTS conducts basic checks of issuing bodies' compliance with the regulations but does not

[7] Second Reading Speech, *AusCheck Bill 2006*, House of Representatives Hansard, 7 December 2006, p. 12.

assess their processes or systems in a systematic way. OTS has the ability, through more focused compliance activity, to gain further assurance around the procedures and practices adopted by issuing bodies as well as the accuracy of the various databases.

Compliance activities

32. The security arrangements for Australian aviation and maritime environments place responsibility on every industry participant to comply with relevant security plans. OTS has established a compliance framework for the ASIC and MSIC schemes that is primarily focused on compliance by high-risk industry participants and issuing bodies. This framework includes a range of audit, inspection and stakeholder activities. The ANAO's examination of 46 high-risk industry participants indicated that the planned compliance activities had occurred. However, there was some inconsistency in practices between OTS offices, which OTS has taken action to address. OTS is also not making the best use of the substantial amount of information it holds about industry participants obtained from its audit, inspection and stakeholder programs to refine and inform its compliance activities.

33. OTS has a compliance regime in place that aims to cooperatively encourage compliance through education and audit activities. It regularly identifies examples of non-compliance, such as the improper display of ASICs and MSICs, as well the lack of supervision of VIC holders, suggesting that education activities have not been fully effective.[8] While isolated instances of non-display of cards is an ongoing issue, the ANAO observed general compliance during site visits to 29 different security controlled areas across seven states/territories in Australia.

34. The ATS Act and MTOFS Act provide for an enforcement regime for non-compliance that includes a range of options that can be used as an alternative to, or in addition to, criminal prosecution, however, these powers have not been used. The emphasis has been on education activities only. OTS is developing an enforcement capability which, if effectively implemented, will assist OTS to deliver a graduated range of responses to address non-compliance.

[8] During fieldwork, the ANAO also observed instances of non-display of ASICs and MSICs, as well as the lack of supervision of a VIC holder.

35. The non-return of expired and cancelled cards is a further example of non-compliance that has been an ongoing issue for many years. The evidence suggests that the current method of educating cardholders of their obligations has not been fully effective. The ANAO's analysis of the OTS data indicates that, for 2009–10, the rate of cancelled or expired cards not being returned to the issuing body was:

- ASIC scheme—12 100 from a population of 40 652 (30 per cent); and
- MSIC scheme—601 from a population of 2225 (27 per cent).

The long history of the non-return of expired and cancelled cards suggests that stronger administration or policy solutions should be considered by OTS to improve the rate of return of these cards by issuing bodies.

36. Within the aviation sector, the VIC scheme allows supervised visitors to enter the secure areas of an airport without a background check. The ANAO's analysis has highlighted examples of the substantial use of VICs by individuals as a means to regularly access secure areas of an airport. In 2009–10, based on available data at a selected major airport, around 40 000 VICs were issued at one delivery gate and around 90 per cent of the VICs issued were to individuals who had multiple visits. While VIC holders are required to be supervised, these individuals are using the VIC scheme to gain access to secure areas without the assurance provided by a background check. OTS has been aware of weaknesses in the VIC scheme and has developed proposed regulatory changes to tighten the provisions for visitor management. Due to potential legal impediments, OTS relied primarily on industry advice rather than analysing actual VIC usage to inform these proposed changes. Going forward, determining baseline data and regularly reviewing airport data on the actual usage of VICs would assist OTS in assessing the effectiveness of the changes to the VIC scheme.

Summary of agency responses

Attorney-General's Department

37. The Attorney-General's Department welcomes this report by the ANAO, and will work closely with the Office of Transport Security in implementing any changes. AusCheck is keen to work with the Issuing Bodies to enhance their understanding of the operation of the AusCheck System and using it to meet obligations under the relevant regulations. AusCheck is also committed to increasing use of the Card Verification System—which provides

an online way to verify the authenticity of an individual's ASIC or MSIC—and how it can be accessed and used by ports and airports.

Department of Infrastructure and Transport

38. The Department of Infrastructure and Transport (DIT) welcomes the ANAO Performance Audit into the management of the ASIC and MSIC schemes, and notes positive comments made about a range of matters including DIT's approach to risk management, governance and industry consultation. As part of our on-going continuous improvement process, DIT will continue to working closely with our partner agencies and industry stakeholders to further refine the ASIC and MSIC schemes to better meet the Government's policy objective of providing an efficient, sustainable, competitive, safe and secure transport system.

Recommendations

Recommendation No.1

Para 3.26

To strengthen the ASIC and MSIC schemes, the ANAO recommends that OTS:

(a) reviews the risks arising from the administrative practices of issuing bodies, particularly in the issuing and manufacture of cards, and evidence of the confirmation of an applicant's identity; and

(b) uses the outcomes of the review to assess whether the current arrangements provide an appropriate level of assurance that the schemes' requirements are being met.

DIT Response: *Agreed*

Recommendation No.2

Para 5.23

To provide increased assurance and improve the outcomes of its compliance activities, the ANAO recommends that OTS:

(a) increases its use of information obtained from its audit, inspection and stakeholder programs to focus future compliance activities on areas that represent the greatest security risk; and

(b) captures and shares elements of better practice identified through their compliance activity with industry participants.

DIT Response: *Agreed*

Recommendation No.3

Para 5.52

To improve the effectiveness of the ASIC scheme, the ANAO recommends that, following implementation of the revised visitor management regulations, OTS monitors the actual usage of visitor identification cards at security controlled airports and uses this information to inform the ongoing development of the ASIC scheme and compliance activity.

DIT Response: *Agreed*

Audit Findings

1. Background and Context

This chapter provides background and context on the Aviation and Maritime Security Identification Card schemes. It also outlines the audit approach including the objective, scope and methodology.

Introduction

1.2 The aviation and maritime industries are integral to Australia's interaction and trade with other countries. In 2009–10 there were over 127 million passenger movements through Australian airports, and in 2008–09, over 938 million tonnes of cargo moved across Australian wharves. Since the terrorist attacks in the United States in 2001, there has been an increased range of measures introduced to protect the transport sector against unlawful interference and terrorism. In Australia, the varying measures introduced have sought to enhance the existing 'layers of security' of the aviation and maritime industries.

1.3 The Aviation and Maritime Security Identification Card schemes (ASIC and MSIC schemes) form part of the Australian Government's security measures designed to safeguard the aviation and maritime industries.[9] ASICs and MSICs are displayed by individuals to demonstrate that the holder has had their background checked and are permitted to be in the 'secure areas' of aviation and maritime zones (typically specific parts of airports, seaports and offshore facilities, such as oil and gas rigs).

1.4 ASICs and MSICs are generally required by a range of people who work in secure zones, including: airline staff; airport service workers; baggage handlers; port service workers; stevedores; and transport operators such as train and truck drivers. The aim of the schemes is to: safeguard against unlawful interference with Australia's aviation, maritime transport and offshore facilities; and to reduce the risk of terrorist infiltration.

[9] Australia's current approach to transport security relies on activities across the following complementary layers: intelligence to identify threats; targeted mitigation strategies at last ports of call (the point of departure) to detect and interdict risks before they depart for Australia; law enforcement measures; security measures at airports, seaports and offshore facilities, including preventive physical and identity security measures and access control; passenger, baggage and cargo screening; and aircraft, ship and offshore facilities security. Commonwealth of Australia, *Counter-Terrorism White Paper*, 2010.

1.5 ASICs were first introduced as an industry responsibility in 1998, covering major airports. In March 2005, revised laws extended the scheme to cover security controlled airports with regular public transport.[10] MSICs, which cover security regulated maritime zones, were phased in from October 2005 with full implementation on 1 January 2007.

The ASIC and MSIC schemes

1.6 The ASIC and MSIC schemes were established by the *Aviation Transport Security Act 2004* (ATS Act), the Aviation Transport Security Regulations 2005 (ATS Regulations), and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFS Act) and Maritime Transport and Offshore Facilities Security Regulations 2003 (MTOFS Regulations). This regulatory framework seeks to safeguard aviation, maritime transport and offshore facilities against unlawful interference. Central to achieving this objective is the obligation for industry participants to develop and comply with security plans. The *AusCheck Act 2007* and the AusCheck Regulations 2007 establish the regulatory framework for coordinating and conducting certain criminal, security and other background checks.

1.7 While there are differences in how the ASIC and MSIC schemes operate, they share a common framework in how they are structured. This includes:

- the criteria for obtaining an ASIC or MSIC;
- authorities for issuing ASICs and MSICs;
- the requirement to properly display ASICs and MSICs in secure zones;
- the establishment of 'security regulated' zones; and
- the development of transport and maritime security plans.

1.8 These key elements of the ASIC and MSIC schemes are outlined below.

[10] Regular public transport operation is defined in the Aviation Transport Security Regulations 2005 (Regulation 1.03) as an operation of an aircraft for the purposes of the carriage of people, or both people and goods, of an air service that: (a) is provided for a fee payable by persons using the service; and (b) is available to the general public on a regular basis; and (c) is conducted in accordance with fixed schedules to or from fixed terminals over specific routes.

Criteria for obtaining an ASIC or MSIC

1.9 The ATS and MTOFS Regulations prescribe a range of conditions for the use of the cards and the eligibility criteria for obtaining an ASIC or MSIC. Table 1.1 outlines the key criteria for obtaining an ASIC or MSIC.

Table 1.1

Criteria for obtaining an ASIC and MSIC

Criteria	Description
Operational need	Aviation—a person who has a need for frequent access to a secure area relating to the operation of an airport or an aircraft; and Maritime—if occupation or business interests require or will require unmonitored access to a maritime security zone at least once a year.
Identity verified	An individual's identity is verified primarily through the production of credentials.
Criminal history	The person does not have an adverse criminal record.
Security assessment	The person is not the subject of an adverse security assessment.[11]
Citizenship/ immigration	Aviation—either an Australian citizen or the issuing body is satisfied that the person is not an unlawful non-citizen; and Maritime—either an Australian citizen or valid visa to work in Australia.

Source: ATS and MTOFS Regulations.

1.10 While there are differences in the citizenship/immigration criteria, historically the main practical differences between ASIC and MSIC eligibility criteria were the types of criminal convictions that prohibited a person from holding either an ASIC or MSIC.[12] Appendix 2 lists the aviation and maritime-security-relevant offences. On 1 July 2010, amendments to the MTOFS Regulations more closely aligned the two schemes, noting each scheme still has industry-specific offences as part of the criteria.

1.11 The 'criminal history' criterion is predominantly focused on counter-terrorism and other unlawful acts. As a consequence, individuals with other

[11] The definition of 'security assessment' under both the ATS and MTOFS Regulations has the same meaning as in Part IV of the *Australian Security Intelligence Organisation Act 1979*.

[12] A person will be found to have an adverse criminal record under the ASIC scheme, if they have been convicted and sentenced for (either): two or more aviation security-relevant offences (ASROs), with one occurring in the last 12 months; or one or more ASROs, where they received a term of imprisonment. A person will be found to have an adverse criminal record under the MSIC scheme if they have been convicted and sentenced for one or more maritime-security-relevant offence, where they received a term of imprisonment. A person will also be found to be disqualified from holding an MSIC if they have been convicted of one or more disqualifying offence.

criminal histories are still eligible for an ASIC or MSIC. For example, based on 2009–10 applications, approximately seven per cent of all ASIC applicants and 20 per cent of all MSIC applicants had a disclosable criminal history, which did not preclude the applicant from obtaining an ASIC or MSIC.

Issuing bodies

1.12 Issuing bodies are organisations that are authorised by the Secretary of Department of Infrastructure and Transport (DIT) to issue ASICs or MSICs in accordance with an issuing body plan.[13] The primary purpose of issuing body plans is to set out procedures for the:

- production, issue, cancellation and return of ASICs and MSICs;
- safekeeping of ASICs and MSICs; and
- associated equipment and maintenance of records kept in relation to applicants.

1.13 A range of entities can become issuing bodies, including airport operators, and aviation and maritime industry participants. In practical terms this includes airline carriers and port authorities. As at 1 February 2011, there were 182 ASIC issuing bodies and 20 MSIC issuing bodies. A list of the issuing bodies can be found in Appendix 3.

1.14 Issuing bodies have a range of requirements under the ASIC and MSIC schemes, including:

- verifying the identity of applicants;
- confirming the operational need for a card;
- various record keeping responsibilities; and
- the production and destruction of cards.

Display of ASICs and MSICs

1.15 A person must hold and properly display a valid ASIC or MSIC if he or she is to work in a designated security zone. There is a range of exceptions and

[13] Under the ATS regulations issuing bodies are required to develop and give effect to ASIC programs (ATS Regulation 6.07). Under the MTOFS regulations issuing bodies are required to develop and give effect to MSIC plans (MTOFS Regulation 6.07R). For the purposes of this report the term 'issuing body plan' covers both ASIC programs and MSIC plans.

provisions for visitors, emergency personnel and certain government personnel.

1.16 ASICs or MSICs must also be 'properly displayed'. This requires the entire front of the card to be clearly visible and above waist height at the front or side of the body. The potential penalty for the improper display of a valid ASIC or MSIC is currently set at $550. Figure 1.1 is an example of an industry participant's efforts to promote the proper display of an ASIC.

Figure 1.1

Example of signage promoting the proper display of an ASIC

Source: ANAO.

ASICs

1.17 ASICs can be issued as either a red or grey card depending on the type of access required by the individual. Generally, a red card is required for 'airside' access, particularly close to the terminal; whereas either a red or grey card is required for 'landside' access. The difference between the terms airside and landside is discussed in paragraph 1.23. The ATS Regulations also prescribe rules for the display and issuing of visitor identification cards (VICs), for supervised visitors within secure zones.

1.18 ASICs generally expire after two years, but shorter periods apply for people under the age of 18, people with discretionary ASICs and temporary cards.[14] Issuing bodies are also able to issue ASICs to applicants under the age of 18 without a background check. Temporary cards can be issued to those whose cards have been mislaid, destroyed, lost or stolen.

1.19 ASICs are issued as either Australia-wide or airport-specific. An airport-specific ASIC has validity only at the airport specified on it.

MSICs

1.20 The MTOFS Regulations do not prescribe different coloured cards depending on the zone to be accessed. All MSICs are legislatively prescribed blue in colour. In contrast to the ASIC scheme, there is also no requirement for supervised visitors in a maritime security zone to display a card.

1.21 Historically, MSICs were valid for a period of five years from the date of the background check. However, from 1 December 2010, the maximum MSIC validity period was reduced from five to four years; and a background check will be required every two years. Similar to the ASIC scheme, a temporary MSIC can be issued to a holder who has forgotten the card or if it has been lost, stolen or destroyed. Issuing bodies are also able to issue MSICs to applicants under the age of 18 without a background check. However, the MSIC ceases to be valid six months after the holder turns 18. The concept of airport-specific ASICs has no equivalent in the MTOFS Regulations.

[14] Applicants who do not satisfy the initial criteria for an ASIC can apply for a discretionary ASIC. The process of discretionary ASICs allows the Secretary of DIT to issue cards with conditions; the most common condition is a restriction on the validity period of the card. Discussed further in Chapter 3.

The establishment of security controlled zones

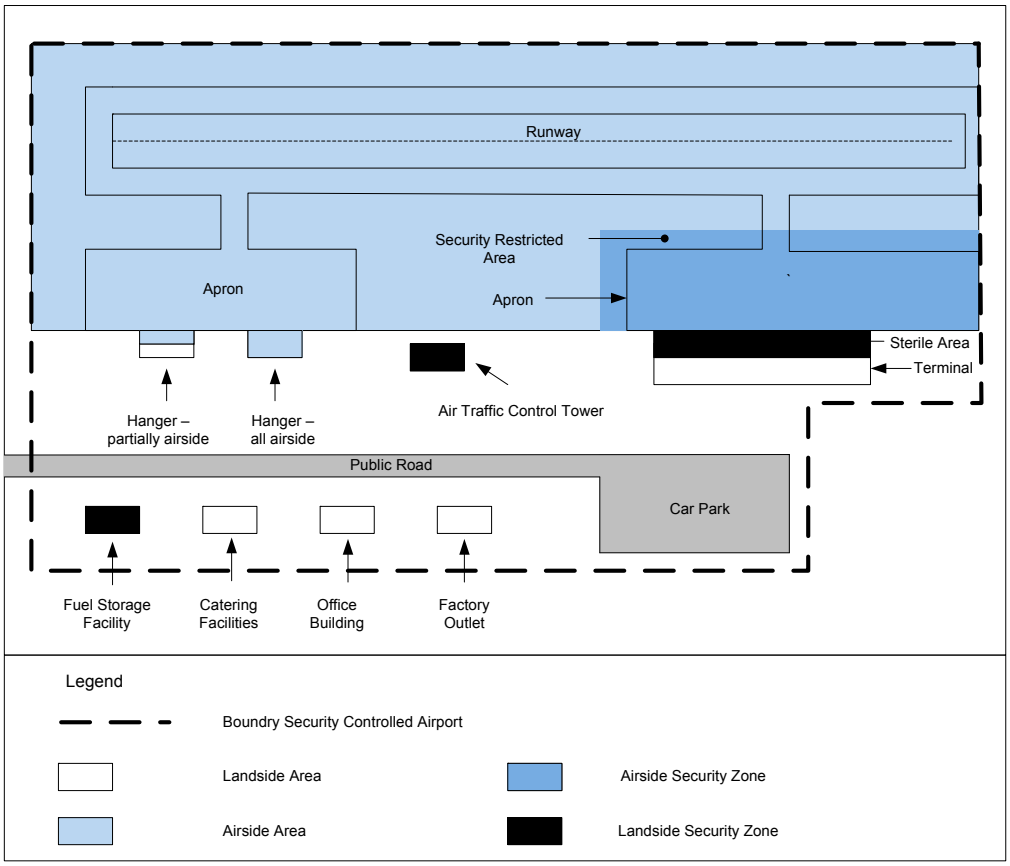
1.22 The establishment of security controlled areas[15] are prescribed by the ATS and MTOFS Acts. It is within security controlled areas that security controlled zones are created with additional security requirements, which may include the display of ASICs and MSICs. Aviation and maritime security zones can be established by the Secretary of DIT within a security controlled airport; a security regulated port; and on and around a security regulated offshore facility. The MTOFS Act also regulates that certain ships automatically classify as security regulated ships if they meet certain criteria.

1.23 Under the ATS Act, the Secretary has the power to declare particular airports as security controlled airports and to establish airside and landside areas of these airports. The Secretary may also declare airside and landside security zones within airside and landside areas. It is these airside and landside zones that are generally subject to the additional security requirement of displaying an ASIC. As is shown in Figure 1.2, only specific areas within a security controlled airport require a valid ASIC to be displayed.

[15] For the purposes of this report, 'security controlled area' includes a security controlled airport; a security regulated port; and a security regulated offshore facility.

Figure 1.2

Diagram of a typical security controlled airport.



Source: Aviation Transport Security Regulations 2005, Regulation 3.02.

1.24 Under the MTOFS Act, the Secretary of DIT may declare the boundaries of maritime security zones. These zones are used for areas within ports, on and around ships and on and around offshore facilities where additional security is required, including:

- landside restricted zones;
- waterside restricted zones;
- ship security zones:
- on-board ship security zones; and
- offshore oil and gas security zones.

1.25 Broadly, a ship security zone operates around a security regulated ship while it is in a security regulated port or near a security regulated offshore facility. In practical terms, many of the maritime security zones are only activated when a ship is in a port.

1.26 A port may be declared as a security regulated port if it is intended for use either wholly or partly in connection with the movement, loading maintenance or provision of a security regulated ship as established by criteria. Security regulated ships include passenger ships and cargo ships of 500 gross tonnage or more that are used for overseas or inter-State voyages. Passenger ships, such as the ferries in Sydney harbour, are therefore not security regulated ships.

1.27 As at November 2010 there were 177 security controlled airports in Australia (outlined in Appendix 4). While the number of security controlled ships can vary, as at November 2010, there were 73 security regulated ports and 69 security regulated offshore facilities (outlined in Appendix 5).

Security plans

1.28 A further part of the integrated layered security approach is the development and implementation of security plans. Relevant industry participants who operate security controlled areas or particular services related to the security controlled area are required to have a security plan.[16] In practical terms, the relevant industry participants required to have security plans include airports, airlines, port operators, container load operators and freight operators.

1.29 The security plans are approved by the Secretary of DIT and are generally for a five-year period. The content of security plans is prescribed by legislation and, broadly, creates obligations for industry participants to develop and implement a range of security activities and measures that will contribute to the maintenance and achievement of aviation and maritime security outcomes.

1.30 The security plans outline some specific requirements to establish the operation and controls surrounding the ASIC and MSIC schemes, including:

[16] For the purposes of this report 'security plan' includes transport (aviation) and maritime security plans.

- proposed security zones and the planned measures and procedures to monitor and control access to restricted security zones;
- procedures for managing security;
- procedures for quality control including auditing; and
- procedures for physical security and access control.

1.31 The obligation for a variety of industry participants to have security plans also creates a scenario that in certain locations there are multiple 'responsible' industry participants. For example, in Sydney Airport at the time of ANAO fieldwork in October 2010, there were 49 transport security plans in operation (14 tenants and 35 international airlines), and within Sydney Ports there were 13 separate maritime security plans in operation. In practical terms, this creates an environment where security responsibility rests with multiple industry participants as well as the individual. Overall, at the time of the audit there were over 1200 industry participants operating at the various aviation and maritime security regulated zones.

Administrative arrangements

1.32 Responsibility of the ASIC and MSIC schemes rests across numerous Australian Government agencies with varying levels of involvement. The key agencies involved are:

- DIT—administers the ATS Act and MTOFS Act;
- Attorney-General's Department (AGD)—administers the AusCheck Act and coordinates the background checking;
- CrimTrac—coordinates the criminal history checks as part of the background check;
- Australian Security Intelligence Organisation (ASIO)—conducts the security assessments as part of the background check; and
- Department of Immigration and Citizenship (DIAC)—conducts, if required, an unlawful non-citizen or eligibility to work in Australia check as part of the background check.

1.33 Of these key agencies, DIT and AGD play the central roles in administering the ASIC and MSIC schemes.

Department of Infrastructure and Transport

1.34 DIT provides policy advice to the Australian Government on a wide range of transport issues, including those arising in both the aviation and maritime sectors. Within DIT, the Office of Transport Security (OTS), established in 2003, has principal responsibility for administering aviation and maritime security. OTS is the Australian Government's primary advisor on transport security, and acts as the security regulator of the aviation and maritime transport industry. OTS's role is to provide expert advice and regulatory oversight for the Australian Government by taking a risk-based approach to continually enhance security in Australia's transport system. OTS seeks to perform this role in consultation with industry and through international engagement.

1.35 In consultation with other agencies, OTS provides:

- risk context advice to industry to inform risk assessment processes; and
- advice on, and conducts reviews of, security policies and legislation, seeking consistency with international obligations.

1.36 OTS's primary role as the transport security regulator is the approval of transport security plans and monitoring compliance with approved plans. In relation to the ASIC and MSIC schemes, OTS approves ASIC programs and MSIC Plans, on behalf of the Secretary, and monitors the compliance of industry participants, issuing bodies and cardholders.

Attorney-General's Department

1.37 The role of AGD is to provide expert support to the Government in the maintenance and improvement of Australia's system of law and justice and its national security and emergency management systems. AusCheck is a branch within AGD, established in 2006, which administers the AusCheck Act and the AusCheck Regulations. Its role is to conduct the background checking component of the broader procedures under which ASICs and MSICs are issued (or refused). This background check potentially includes three checks:

- a criminal records check coordinated by CrimTrac;
- a security assessment by ASIO; and
- a citizenship/immigration check conducted by DIAC, if relevant.

1.38 AusCheck does not set the criteria against which the checks are conducted; this is established by the criteria within the ATS and MTOFS Regulations. AusCheck also does not make the final determination whether or not to issue a person an ASIC or MSIC—subject to the AusCheck advice, this decision rests with the issuing body. AusCheck coordinates the checking process and makes an assessment of the security risk posed by the applicant. AusCheck's assessment is by way of advice to the issuing body. The AusCheck finding will generally be either:

- a statement that the individual meets the statutory criteria specified for the background check; or
- a 'qualified response', meaning a finding of a 'pattern of criminality', which only allows a person to be issued with a 'conditional' card (only in the case of ASICs)[17]; or
- a direction not to issue a card.

1.39 There are numerous bodies involved in the delivery of the ASIC and MSIC schemes, including both industry organisations and Australian Government agencies. OTS administers the regulatory framework for the ASIC and MSIC schemes on behalf of the Australian Government. AusCheck coordinates the background checks on ASIC and MSIC applicants. As at 30 June 2010 there were 265 328 valid cards (126 806 ASICs and 138 522 MSICs) recorded on the AusCheck database, the consolidated database of all cardholders. In addition to the cardholders, there are over 200 bodies that are authorised to issue the cards and 1200 industry participants regulating access to secure areas where the display of ASICs and MSICs is required. The key responsibilities of the parties involved in the ASIC and MSIC scheme are summarised in Table 1.2.

[17] The condition that must be included on the ASIC is that the person undertakes a further background check within 12 months after the first background check—ATS Regulation 6.28 (7).

Table 1.2

Key ASIC and MSIC responsibilities

Party	Key ASIC and MSIC Responsibility
Industry participants (airports, ports etc)	Developing security plans and ensuring that access to security zones is limited to ASIC and MSIC holders.
Issuing bodies (airports, ports, third party bodies etc)	Issuing ASICs and MSICs only to individuals who have been checked through AusCheck and meet regulatory requirements.
OTS	Approving transport security plans; and monitoring the compliance of industry participants, issuing bodies, and cardholders.
AusCheck	Coordinating background checks on ASIC and MSIC applicants and maintaining the AusCheck database.
Cardholders	Meeting eligibility criteria and displaying ASICs and MSICs in security zones.

Source: ANAO analysis.

Parliamentary and government review

1.40 There has been significant interest in the security of the aviation and maritime industries. Recently, with a particular focus on aviation, this has included the:

- 2004 Joint Committee of Public Accounts and Audit (JCPAA) Report 400–*Review of Aviation Security in Australia*, which included a recommendation surrounding the return of expired cards;
- 2005 *Wheeler Airport Security and Policing Review* (Wheeler review), which was presented to Government and made a range of recommendations, one of which led to the establishment of AusCheck as the centralised agency coordinating background checking;
- 2005 JCPAA Report 406–*Developments in Aviation Security since the Committee's June 2004 Report 400: Review of Aviation Security in Australia–An Interim Report*, which made a series of recommendations towards tightening the process for issuing visitor identification cards (VICs); and
- 2006 JCPAA Report 409–*Developments in Aviation Security Since the Committee's June 2004 Report 400: Review of Aviation Security in Australia*, which made further recommendations surrounding the ASIC scheme, including VICs; and

- *National Aviation Policy White Paper: Flight Path to the Future,*[18] released in 2009, and included a commitment to strengthening the ASIC scheme.

1.41 In responding to these reports, the Government has been largely supportive of the recommendations and suggestions. Changes to the regulatory framework with the introduction of the ATS Regulations 2005 mandated the identification by issuing bodies of their processes to manage the retrieval of expired cards. A proposal to tighten the process for issuing VICs, was also agreed to by the Minister for Infrastructure and Transport in February 2011, with full implementation planned to take effect in late 2011 (discussed in Chapters 2 and 5).[19]

1.42 On 14 September 2009, the Parliamentary Joint Committee on the Australian Crime Commission initiated an inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime pursuant to Section 55(1)(d) of the *Australian Crime Commission Act 2002*. One of the terms of reference is the effectiveness of the ASIC and MSIC scheme as a means of addressing serious and organised crime. On 25 November 2010, the Committee's name was changed with the commencement of the *Parliamentary Joint Committee on Law Enforcement Act 2010* to become the Parliamentary Joint Committee on Law Enforcement (PJCLE). As at March 2011, the PJCLE has received submissions and taken evidence through public hearings.

Audit approach

Audit objective and scope

1.43 The objective of the audit was to assess the effectiveness of DIT's and AGD's management of the ASIC and MSIC schemes.

1.44 The ANAO identified four key areas for review:

- governance, reporting and funding arrangements;
- processes for issuing ASICs and MSICs;
- information management; and
- compliance activities supporting the ASIC and MSIC schemes.

---

[18] Commonwealth of Australia, *National Aviation Policy White Paper: Flight Path to the Future*, 2009.

[19] Broadly, the agreed principals of the proposed VIC model include: setting a maximum aggregate period of days in a 12 month period that VICs can be issued to a person, requiring photo identification to be provided, and requiring a record of the reason for issuing the VIC.

1.45 The audit was focused on the activities of DIT and AGD. The activities of CrimTrac, ASIO or DIAC in relation to the ASIC and MSIC schemes were not assessed in this audit.

Methodology

1.46 To achieve the audit objectives, the audit methodology included:

- interviews with OTS and AusCheck staff and external stakeholders;
- a range of site visits across seven states/territories to 29 security controlled areas across Australia;
- file and document reviews; and
- specific IT audit testing of the AusCheck database.

1.47 The ANAO also worked closely with a range of issuing bodies that provided de-identified data of their individual registers. This data was used for a range of analyses, including data matching with the AusCheck database.

1.48 The audit was conducted in line with the ANAO's auditing standards at a cost of approximately $420 000.

2. Governance Arrangements for the ASIC and MSIC Schemes

This chapter examines the governance arrangements for DIT's and AGD's management of the ASIC and MSIC schemes.

Introduction

2.1 Governance refers to the processes by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised in the organisation.[20] The ANAO assessed the effectiveness of DIT's and AGD's governance arrangements for the ASIC and MSIC schemes. In particular, this assessment included: the organisational structure; risk management and review; monitoring and reporting; financial management; and stakeholder consultation.

Office of Transport Security—DIT

2.2 The ASIC and MSIC schemes are one component of OTS's broader responsibilities associated with the ATS and MTOFS Acts. OTS's primary role in the management of the ASIC and MSIC scheme is monitoring the extent to which industry participants, issuing bodies and cardholders comply with legislative and regulatory requirements. OTS also has responsibility for managing the following aspects of the schemes:

- setting of regulatory standards;
- provision of policy guidance to industry;
- assessing issuing bodies' ASIC programs and MSIC plans for consideration of approval;
- assessing applications from ASIC and MSIC applicants after they are initially refused an ASIC or MSIC;
- assisting issuing bodies to comply with their annual reporting obligations; and

[20] ANAO Better Practice Guide—*Public Sector Governance*, July 2003, Canberra.

- assessing requests for exemptions from holding, carrying or displaying an ASIC or MSIC.

Organisational structure and risk management

2.3 Primary responsibility for the ASIC and MSIC schemes sits between two branches within OTS. There are clear accountability arrangements for each branch that are reflected in branch planning documents. The implementation of OTS's regulatory function is overseen by OTS's Policy and Audit Committee (OPAC). The role of OPAC includes identifying transport security policy 'best practice' and lessons learned for wider application within the business of OTS. The committee also reviews and confirms, on a quarterly basis, the National Audit and Compliance Program.

2.4 OTS has implemented an appropriate organisational structure that allows it to implement, monitor and coordinate tasks and deliverables. DIT also has an established risk management framework that is monitored and overseen by its Audit Committee. Risks are systematically assessed and managed at a departmental, divisional and branch level using a standard risk management methodology. Key operational risks were documented and updated in OTS's risk register, and had clear mitigation strategies. There was also high-level monitoring of risks. For example, senior managers are required to document in their Branch Business Plan how their branch will manage and mitigate key risks.

ASIC and MSIC review

2.5 The ASIC and MSIC schemes have undergone a number of changes since their inception. These changes have been driven by a range of factors, including Parliamentary as well as internally commissioned reviews. The ANAO assessed the processes adopted by OTS in implementing recommended changes to the ASIC and MSIC schemes.

ASIC review

2.6 The ASIC scheme commenced in 1998 with a relatively simple criminal history background check conducted once every five years. Established under the *Air Navigation Act 1920*, the ASIC scheme was designed to mitigate vulnerabilities related to the use of 'trusted insiders' who may facilitate terrorism or unlawful interference against aviation. Since its commencement, there has been an incremental but significant strengthening in the background checks being undertaken, the eligibility criteria applied, the frequency of checks, and the security features on the card itself.

2.7 As highlighted in Chapter 1, throughout the history of the ASIC scheme there have been a range of reviews and government commitments that have touched on aspects of ASICs. This has included JCPAA reports, the Wheeler review in 2005, as well as the *National Aviation Policy White Paper: Flight Path to the Future* (White Paper) in 2009.[21] The JCPAA reports have made a series of recommendations surrounding the ASIC scheme. In particular, the most recent aviation-related report, the 2006 JCPAA Report—409,[22] recommended:

- any decision by AusCheck should be subject to appeal through the Administrative Appeal Tribunal;
- the centralisation of issuing ASICs through AusCheck;
- a detailed and formal mechanism for the return of expired cards; and
- a tightening of the VIC scheme, including a tightening of conditions to ensure VICs are provided for genuinely temporary purposes.

2.8 The Government responded to these recommendations in 2008 with general support or support with qualifications. The Government response noted an internal ASIC legislative review which was seeking to assess ASIC eligibility criteria and the proposal for AusCheck to become responsible for the issuing of all ASICs. It was suggested by Government that the ASIC legislative review would form the basis for proposed changes.

2.9 The finalised 2008 ASIC legislative review highlighted: vulnerabilities in the robustness and timeliness of background checks, proof-of-identity checks, and the management of visitors in the secure zones of Australian airports. The review made a number of key structural recommendations and suggested a proposed implementation plan to address the risks identified in the review. In September 2008, the then Minister for Transport, Regional Development and Local Government was advised of these findings and noted the proposed future course of action. For example, subject to additional funding, it was proposed that:

---

[21] Commonwealth of Australia, *National Aviation Policy White Paper: Flight Path to the Future*, 2009.

[22] JCPAA Report 409–*Developments in Aviation Security Since the Committee's June 2004 Report 400: Review of Aviation Security in Australia.*

- there would be a removal of all issuing bodies in the current form, requiring individuals to apply directly to government, which would centralise the issuing of all cards;
- a severing of the links between background checking and the granting of access to the secure areas of airports; and
- a centralisation of identification checking in a manner similar to that used by the Australian Passports Office.

2.10 Simultaneous to the 2008 ASIC legislative review, the then Government was in the process of developing the White Paper. To support this, OTS had developed an issues paper '*Towards a National Aviation Security Policy'*, which was issued for consultation purposes in April 2008. The Government's aviation green paper followed the issues paper and was issued in December 2008 after the completion of the 2008 ASIC legislative review. The green paper made mention of the 2008 ASIC legislative review and said that recommendations contained in the review would be considered by the Government in the near future. Ultimately, some elements of the 2006 JCPAA Report—409 and 2008 ASIC legislative review were incorporated into the White Paper. The recommendation by the JCPAA in its 2006 report to centralise the issuing of ASICs was not progressed. OTS advised that this proposal is still subject to ongoing consideration.

2.11 The White Paper was issued in December 2009 and included a commitment to strengthening the ASIC scheme. The then Government committed to enhancing the ASIC scheme by:

- strengthening the cancellation provisions for ASIC issuing bodies;
- making provision for subsequent background checks for ASIC holders where their eligibility may have changed;
- increasing the maximum penalty for an ASIC holder failing to report that they have been convicted of an aviation security relevant offence; and
- tightening the provisions for visitor management at security controlled airports.

2.12 Administratively, it was proposed that the ASIC regime would be streamlined by reducing the number of issuing bodies and enabling ASIC applicants to apply directly to the Secretary of DIT for a discretionary ASIC, rather than discretionary ASIC applications being submitted by an issuing

body as the sponsor of the ASIC applicant. Also proposed were changes to the: display of expiry dates; expansion of ASIC display exemptions; and issue of replacement cards to individuals who had already had a current background check.

ASIC Enhancement Project

2.13 OTS developed a planning methodology to implement the enhancements outlined in the White Paper. This involved consultative mechanisms as well as a series of policy/discussion papers that were provided to industry participants including an *ASIC Implementation Issues Paper* in March 2010.

2.14 During these consultative phases, industry participants noted, among other issues, concerns about the practicality of some of the proposed changes, the potential cost involved in implementing the proposed changes, as well as the long lead time required to implement any changes for many of the larger industry participants. In June 2010, OTS gained approval from the then Minister for Infrastructure, Transport, Regional Development and Local Government to a range of regulatory changes to give effect to the commitments made in the White Paper with a phased rollout of implementation of the enhancements to start from 1 August 2010.

2.15 The first phase of the changes commenced on 1 December 2010.[23] Subsequent consultation with industry participants confirmed the practical difficulties in implementing some of the proposed changes, and the caretaker period surrounding the 2010 general election had also resulted in delays. A new proposal was agreed to by the Minister for Infrastructure and Transport in February 2011. The proposed changes seek to limit the aggregate number of days that VICs can be issued to an individual at a specific airport in a 12 month period, with full implementation planned to take effect in late 2011.

2.16 While the proposals in the White Paper seek to address some identified vulnerabilities (as observed by the ANAO, and highlighted in some of the findings of this audit) some of the underlying risks identified in the original reviews still remain, and will continue to exist with the proposed changes. For

[23] These included changes to: ASIC holders reporting convictions; suspension of ASICs; subsequent background checks; ASIC cancellation provisions; applications for discretionary ASICs; replacement ASICs; AusCheck database and issuing body registers; ASIC expiry date; and ASIC display exemptions.

example, a consequence of the structure of ASIC and MSIC schemes with multiple issuing bodies reduces the assurance of the total number of current cards, or the currency of all cards on the AusCheck database (discussed in Chapter 4). Further, in at least one airport, ANAO analysis has shown that the proposed tightening of the visitor regime, by setting a maximum aggregate period of days in a 12 month period that VICs can be issued to a person, will not prevent a large number of individuals who are using the VIC scheme in a systematic manner to continue to gain regular access to secure areas (discussed in Chapter 5).

2.17 Consequently, it will be important for OTS to closely monitor and assess the outcomes of the implementation of changes to the regulatory scheme and to provide advice to Government about refinements to the current policy, as is considered necessary.

MSIC Review

2.18 OTS commissioned an external review of the MSIC scheme in 2009. The report *Assessment of Maritime Security Identification Card (MSIC) Eligibility Criteria* (MSIC report) completed in June 2009 focused on whether the scheme was meeting policy objectives. The report found that the eligibility criteria did not capture the range of offences and behaviours that are known to have linkages with terrorist activity and the unlawful interference with maritime transport and offshore facilities.

2.19 To address some of the issues identified in the MSIC report, in January 2010 the Australian Government announced a range of proposed measures, including:

- increasing the number of categories of criminal offences that preclude an applicant from obtaining the necessary background clearance (from 137 to 298 categories);
- requiring all MSIC holders to undergo a compulsory criminal history check and ASIO security assessment every two years, instead of five years; and
- the maximum MSIC validity period was reduced from five to four years.

2.20 OTS has consulted appropriately with industry and the issues raised have been considered in developing amendments to the legislation and regulations. These consultations included working group meetings that sought to resolve practical implementation issues, including a phased approach to

regulatory changes as well the distribution of discussion papers. As a result of this process, the MTOFS Regulations were amended on 30 June 2010.

2.21 The first element of the MSIC enhancements came into effect on 1 July 2010. This included new offence categories in the MSIC eligibility criteria. All new MSIC applications and renewals are background checked against the new offence categories. On 1 December 2010 the card validity, suspension provisions, further additional background checking requirements and the new offence categories for MSIC holders and issuing bodies took effect.

Stakeholder engagement

2.22 Given the large number of industry participants as well as issuing bodies, stakeholder consultation plays an integral role in the successful operation of the ASIC and MSIC schemes. OTS consults with industry participants and employees through a range of meetings and forums including the:

- Aviation Security Advisory Forum (ASAF);
- Regional Industry Consultative Meeting (RICM);
- Aviation Security Employee Consultative Forum (ASECF);
- Maritime Industry Security Consultative Forum (MISCF);
- Maritime Security Identity Card Implementation Working Group;
- ASIC Key Stakeholders Working Group Meetings; and
- the Australian Government Transport Security Policy Committee (AGTSPC).

2.23 Attendance and participation at these forums forms a significant component of OTS activities and consultation with the industry. In addition to the more strategically focused forums listed above, OTS is also involved at the local level at aviation and maritime location-specific security forums.

2.24 The arrangements in place for OTS stakeholder consultation are appropriate, given the large number of industry participants and the diversity of perspectives of participants.

Monitoring and reporting

2.25 Monitoring and reporting the outcomes of compliance activities is an important element of an agency's accountability to key stakeholders, such as the Minister, industry participants and the general public. OTS reports quarterly to DIT's executive on compliance activities in line with its National Compliance Program (NCP). These reports provide information on all findings of non-compliance and align the findings with identified risks that have been developed by OTS and draw on classified intelligence from the Australian intelligence community.

2.26 OTS records information gathered through its compliance activities on dedicated databases. This information is used to: further develop its compliance scheme; determine emerging trends at the local and national level, which may require additional compliance activity to be undertaken; and provide statistical reporting to OTS Executive.

2.27 OTS has established an appropriate framework for the monitoring and reporting of compliance activities. It reports regularly to industry on the results of its NCP through regular consultative meetings held with industry participants. For example, an update on the NCP is a standing agenda item at the ASAF, RICM and MISCF. The ANAO reviewed a sample of reports and observed that they are presented by the Executive Director of OTS and cover: the volume and coverage of compliance activity during the financial year; the number of non-compliance findings; key issues; trends; and emerging aviation and maritime vulnerabilities.

AusCheck—AGD

2.28 AusCheck is a branch in the National Security Law and Policy Division within the AGD. It coordinates background checking and vets applicants for ASICs and MSICs, and maintains a database containing information on all applicants, as well as those people who ultimately are issued with a security identification card.[24] AusCheck seeks to apply a consistent interpretation of statutory requirements, coordinates criminal and security checks on applicants and notifies the relevant bodies on the outcome of these checks. Information from the database can, in certain circumstances, be provided to authorised national security and law enforcement agencies.

[24] *AusCheck Act 1997*, s 14(1).

Financial Management

2.29 AusCheck was established as a cost recovery agency. Under the cost recovery policy, regulatory agencies are expected to have in place arrangements to provide assurance that they are charging the correct amount under cost recovery schemes. Industry and other customers expect assurance that the fees and charges they are paying are fair, and reflect only those costs incurred in the provision of the activity.

2.30 AusCheck's principal source of revenue is from a fee levied on issuing bodies for services related to background checking. This includes specific components for the CrimTrac and ASIO check (and potentially the DIAC check), as well as the internal costs for processing the background checks.[25] The fee structure of AusCheck's current charges is shown in Table 2.1.

Table 2.1

AusCheck fees

Fees	Cost of background check	Cost of background check with DIAC check
2 year background checking fee for ASICs and MSICs	$81	$85
4 year background checking fee for MSICs	$160	$164

Source: AusCheck.

2.31 The design of AusCheck's fee structure is documented in their Cost Recovery Impact Statement (CRIS). AGD developed a CRIS in 2006 with an intention to promptly review the methodology following initial implementation. Subsequently, a new CRIS was developed and implemented for 2008–2010 and, following consultation, AusCheck released their current CRIS, which operates from 1 July 2010–30 June 2012.

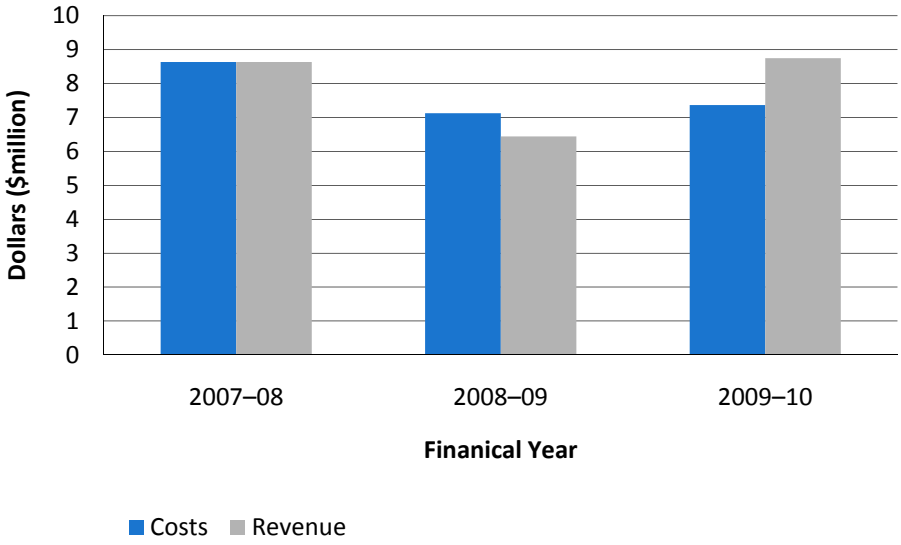
2.32 An inherent difficulty with the early CRIS was the prediction of the number of cards expected to be processed. As a result, there were some variances between the costs and revenue for 2008-09 and 2009–10. Notwithstanding these variances, the ANAO considers AusCheck has established and implemented processes to identify the price structure and cost

[25] The fee charged to applicants varies between issuing bodies dependent on their commercial arrangements. For example, the cost of an ASIC ranges between $180-$196, a two-year MSIC ranges between $215-$234 and a four-year MSIC ranges between $315-$462.

of its regulatory activity over the course of the program's life. Figure 2.1 outlines AusCheck's costs and revenue over the period 2007–08 to 2009–10.

Figure 2.1

AusCheck's costs and revenue 2007–08 to 2009–10



Source: ANAO analysis.

Note: AusCheck was a recipient of an annual appropriation in 2007–08 for part of its revenue.

Stakeholder engagement

2.33 AusCheck also engages in formal and informal stakeholder consultation from day-to-day technical queries through to a peak consultative forum. The main avenues for AusCheck consultation are:

- a client consultative forum;
- publicly available newsletter; and
- client satisfaction survey.

2.34 The consultative forum met frequently during the initial rollout and implementation of AusCheck. The increased contact with issuing bodies was because a range of technical issues emerged and needed to be communicated and resolved. More recent forum discussion items have included photograph lodgement (discussed further in paragraph 3.35), system down time and the development of the renewed CRIS. Feedback received by the ANAO from issuing bodies was generally positive about the level of response and engagement from AusCheck.

2.35 AusCheck has also established processes to assist issuing bodies to comply with their regulatory obligations. For example, AusCheck maintains a web interface to the AusCheck database that allows for the production of reports and updates for issuing bodies processing ASIC and MSIC applications.

2.36 The ANAO observed that the full functionality of the AusCheck web interface was not well understood by all issuing bodies. For example, issuing bodies have the ability to access the AusCheck database and confirm card details, including the name, photograph, card number and location where the card is valid. This capability is designed to allow certain industry participants to confirm the validity and authenticity of a card presented to them. At the time of fieldwork, only five of the 202 issuing bodies had established the functionality to use this third-party verification. While many of the web interface features are described in the available documentation, there would be merit in AusCheck periodically updating issuing bodies about the capabilities of the database.

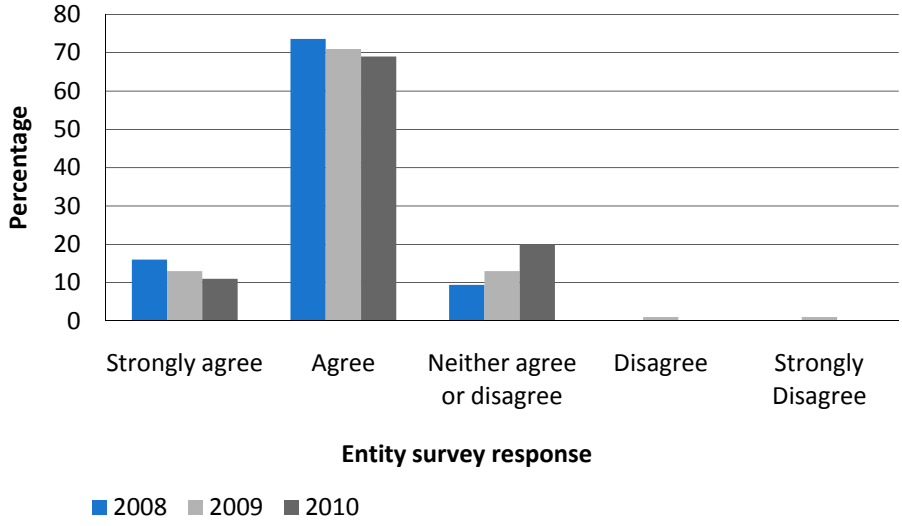
2.37 AusCheck uses its website as a means of providing information to issuing bodies. This includes: AusCheck's privacy policy, a detailed list of frequently asked questions, a service charter and a historical record of past newsletters. In addition to technical updates, the newsletter contains details of the volume of transactions and performance against service levels. AusCheck also runs a helpdesk with access via email, fax or phone and conducts an annual survey to assess client satisfaction and to identify any areas for improvement. Such survey work can provide a basis for the independent view of an entity's service delivery and also act as an avenue for client feedback.

2.38 A key difficulty for AusCheck is managing the perception of what is its responsibility and what is the responsibility of checking partners (ASIO, CrimTrac or DIAC). The survey results to date highlight that this distinction between responsibilities is not always clear to issuing bodies. Many of the less positive responses relate to timeliness issues beyond the control of AusCheck, for example when background checks were being undertaken by background checking partners.

2.39 Figure 2.2 provides the overall client satisfaction level of issuing bodies with AusCheck's services from the last three years.

Figure 2.2

Client satisfaction: AusCheck's services are of a high quality, 2008–2010.



Source: ANAO analysis of AGD data.

Note: Survey responses to the question 'considering all aspects of service, services provided by AusCheck were of a high quality'.

2.40 The effectiveness of AusCheck's broad consultative approach is reflected in the survey results which show that 95 per cent of all issuing bodies surveyed either agreed or strongly agreed that the communication received from AusCheck was relevant to their business needs. This level of satisfaction has been consistent across the years that AusCheck has been in operation, suggesting that the scope and manner of AusCheck's stakeholder engagement is appropriate.

3. The Process for Issuing ASICs and MSICs

This chapter discusses the process for issuing ASICs and MSICs and covers the application process as well as the role, involvement and effectiveness of OTS and AusCheck in conducting background checks and assessments. The process by which individuals whose application has been rejected can apply for a discretionary ASIC or MSIC is also discussed.

Introduction

3.1 As previously noted, issuing ASICs and MSICs involves a number of Australian Government bodies in addition to 202 issuing bodies. The schemes rely on each participant understanding and correctly applying the legislative process. The failure by any body involved in this process to adequately perform their role potentially weakens the integrity of the ASIC and MSIC schemes as a whole.

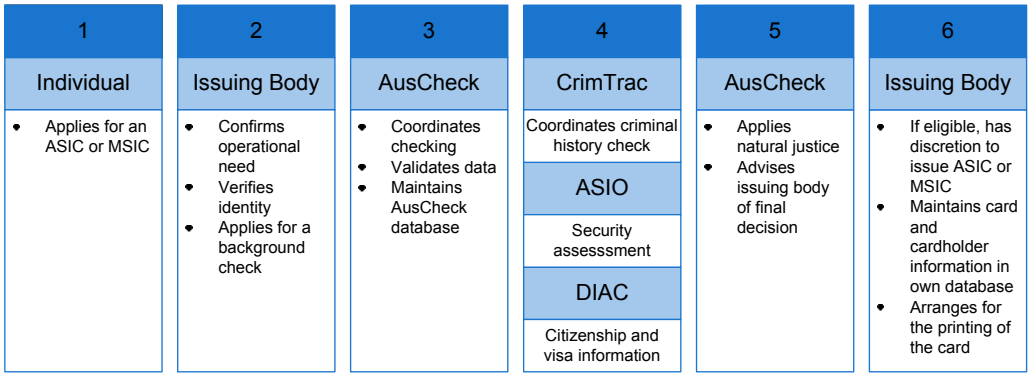
3.2 The devolved nature of the schemes presents particular risks for OTS and AusCheck. While each agency has their individual responsibilities, they must also provide guidance and assistance and gain assurance from issuing bodies. The ANAO examined the assessment of applications and background checking for ASICs and MSICs. The process of applying for a discretionary ASIC or MSIC was also reviewed.

Application process

3.3 The application process involves many parties. Figure 3.1 illustrates a simplified version of the process for issuing an ASIC or MSIC.

Figure 3.1

Simplified ASIC and MSIC application and issue process



Source: ANAO analysis.

3.4 As discussed in Chapter 1 and noted in Figure 3.1, issuing bodies are fundamental to the ASIC and MSIC schemes. Issuing bodies' responsibilities include:

- having an issuing body plan approved by OTS before they may issue a ASIC or MSIC;
- confirming the applicant's identity and operational need for an ASIC or MSIC;
- maintaining a register of all ASIC or MSIC holders as well as auditable documentation; and
- reporting annually on certain criteria about their ASIC or MSIC register, including the number of valid, cancelled and expired cards.

ASIC issuing bodies

3.5 There are 182 ASIC issuing bodies, of which 177 have valid issuing body plans.[26] The number of issuing bodies is a consequence of the legislative framework that automatically deems operators of security controlled airports as issuing bodies. In addition to security controlled airports, aviation industry participants may also apply to become an issuing body. An issuing body must have an issuing body plan approved by the Secretary of DIT in order to function as such.

[26] There were five entities that were automatically deemed to be issuing bodies that subsequently elected not to develop an issuing body plan. These entities did not issue ASICs.

3.6 Having such a large number of issuing bodies poses administrative challenges. For example, at the time of the audit OTS had 176 of the 178 issuing body plans for current issuing bodies.[27] While there are longer term plans to reduce the number of issuing bodies, as identified in the White Paper, it is important that administrative records are complete.

3.7 The structure of the ASIC scheme also allows issuing bodies to issue ASICs to applicants who do not necessarily have a direct employment or geographical connection to the issuing body. This structure has resulted in a small number of issuing bodies producing a high percentage of ASICs. Only 67 of the 182 (37 per cent) ASIC issuing bodies have issued cards. Further, 85 per cent of ASICs are issued by 15 per cent of all active ASIC issuing bodies.

3.8 There were 126 806 ASIC cards registered on the AusCheck database at 30 June 2010. Qantas is the largest issuing body and has issued 38 142 ASICs (30 per cent of all current ASICs), which is significantly more than any of the other issuing bodies. Qantas primarily issues cards to its own employees, but also to contractors who work directly for Qantas. The second largest issuing body is Aviation ID (16 414, 13 per cent of ASICs), which is a commercial company operating from Merimbula Airport. Aviation ID supplies pilots and other airport service companies with their ASICs. In 2010, Aviation ID issued ASICs for 64 other airports.

MSIC issuing bodies

3.9 Unlike the ASIC scheme (where security controlled airports with regular public transport services are automatically deemed to be issuing bodies), any entity, including a port operator, may apply to the Secretary of DIT to become an MSIC issuing body. As a consequence there are only 20 MSIC issuing bodies, most of which are active. As with ASICs, the majority of MSICs are issued by a small number of issuing bodies. The largest MSIC issuing body is 1-Stop Connections, which is the appointed issuing body for two industry participants. There were 138 522 MSIC cards registered on the AusCheck database at 30 June 2010.

[27] OTS was unable to locate two issuing body plans—OTS advised that neither of the issuing bodies with missing plans has issued an ASIC.

Third party issuing bodies

3.10 Third party issuing bodies can be described as issuing bodies that do not have either a direct employment or geographical connection to the applicant, such as for example, Aviation ID and 1-Stop Connections (discussed above). Overall, two ASIC third party issuing bodies have issued 16 932 ASICs (13 per cent of all ASICs) and six MSIC third party issuing bodies have issued 74 811 MSICs (54 per cent of all MSICs). These third party issuing bodies are companies issuing ASICs and MSICs on a commercial basis. Because of the more distant connection to the applicant, third party issuing bodies potentially pose greater risks, through, for example, the use of falsified documents or photographs.

3.11 The ANAO examined all eight of the third party issuing bodies and, in particular, their processes for receiving applications, establishing operational need, proof of identity and issuing cards to applicants. Each of these third party issuing bodies has a public website where people who can demonstrate an operational need can apply for an ASIC and MSIC online. They all have a basic process so that applicants provide original or certified proof-of-identity documentation and a current photo as well as evidence of an operational need.[28] However, there are a number of practices employed by these third party issuing bodies that increase the risks of both cards being used inappropriately, or intercepted for use by a person to whom the card was not issued. These practices reduce the assurance that the schemes' requirements are being met to appropriate standards.

3.12 In reviewing the approaches taken by the third party issuing bodies the following audit observations were made:

- one third party issuing body advised that they understood that an applicant was not required to 'demonstrate' the requirement or provide documented proof that they require a security identification card.[29] Instead, the issuing body relied on the declaration by the individual that they did not make any false statements;

[28] The general requirement of third party issuing bodies for demonstrating operational need is a letter from an applicant's employer on company letterhead or the industry participant with which they are associated.

[29] MTOFS Regulation 6.07R (1) states that 'An issuing body must not fail to give effect to its MSIC plan.' The relevant third party issuing body plan states that 'An applicant for a MSIC must demonstrate an operational need to enter a maritime security zone at least once a year.'

- two issuing bodies, that combined have issued over 19 000 current security identification cards, have no direct contact with the applicant at all during the application process. Applications are lodged online, documentation is accepted through the post and the security identification cards are sent to the applicants via registered post;
- the majority of third party issuing bodies send ASICs and MSICs to applicants through the post. One, as per its issuing body plan, requires applicants to show identification and collect the MSIC from either the issuing body or Australia Post; and
- one issuing body allowed applicants to upload their photograph to the body's website without any third party verification, provided one of the other certified credentials submitted includes a photograph.

3.13 The ANAO observed the following good processes adopted by third party issuing bodies that reduce the potential risks associated with the falsification of either proof-of-identity documentation or applicant photos:

- one issuing body requires applicants to attend an application interview with the issuing body to verify identity, documentation and a current photo;
- six of the issuing bodies require applicants to present proof-of-identify documentation and a photo to be verified directly to the issuing body or to an authorised agent.

3.14 Table 3.1 provides a summary of some of the key processes of third party issuing bodies.

Table 3.1

Summary of processes of third party issuing bodies

Third Party Issuing Body	Does the issuing body have 'direct contact' with applicant?	Are photos 'verified' by issuing body?	Are cards collected by applicant?
Example A	✓	✓	✖
Example B	✓	✓	✖
Example C	✓	✓	✓
Example D	✓	✓	✖
Example E	✖	✖	✖
Example F	✖	✖	✖
Example G	✓	✓	✖
Example H	✓	✓	✖

Source: ANAO analysis of issuing body plans and public websites.

Notes: 'Direct contact' and 'verification' includes issuing bodies or their authorised agents, e.g. Australia Post.

3.15 There are particular risks associated with third party issuing bodies because of their more distant relationship to the applicant. In this context, the ANAO's analysis has identified non-compliance by some issuing bodies with mandatory standards, and a range of processes adopted by others that further reduce the assurance that the schemes' requirements are being met to appropriate standards. While compliance by issuing bodies is assessed by OTS (discussed in Chapter 5), the systematic assessment of the particular risks presented by third party issuing bodies would enable OTS to gain a better understanding of, and further assurance around, the practices employed by these issuing bodies.

Card manufacture

3.16 ASIC and MSIC issuing bodies are also responsible for the arrangements to manufacture the actual cards. The ATS and MTOFS Regulations prescribe the specific format, colour, font and security features of the card. As the card is used as a means of identifying an individual who has had an appropriate background check, both the ATS and MTOFS Regulations

prescribe a tamper-evident feature in the form of a Kinegram.[30] The Kinegram can only be created with the use of specific machines and licensed technology. OTS approves the use of these machines to a range of bodies through a contractual arrangement with the company that makes the specific stamping machines. While the department is not a party to any contract between the machine manufacturer and machine users, OTS does have an ongoing relationship with most entities that use the machines, by virtue of them also being issuing bodies under the ASIC and MSIC schemes. As at December 2010, there were 18 ASIC and eight MSIC Kinegram machines used by 24 entities—23 issuing bodies and one private company.

3.17 A consequence of the small number of entities with Kinegram machines is that these entities print cards for a range of issuing bodies. The ANAO's analysis identified that 37 per cent of all ASIC and MSIC cards are produced by an entity other than the issuing body (12 per cent of all ASICs and 60 per cent of all MSICs). The outsourcing of the printing of the cards creates a risk to the ASIC and MSIC scheme by introducing an additional process outside the direct control of the issuing body. For example, the ANAO was advised by more than one Kinegram machine holder that the process to produce cards for other issuing bodies was based on an email request with an attached photo from the other issuing body—there was no assurance for the card printer that the card applicant had been appropriately identified and background checked. In these circumstances, the card printer did not check the AusCheck number to confirm the issued card was valid. While this is a process that has been approved in various issuing body plans, OTS has not assessed or monitored these processes through its compliance activities in a systematic manner (discussed further in Chapter 5). Given the extent of the outsourcing arrangements, there would be benefits in OTS extending its compliance activities to incorporate these processes.

3.18 Most entities that have a Kinegram machine are also issuing bodies under the ASIC and MSIC schemes. As such, these entities have an ongoing relationship with OTS. However, one of the Kinegram machines is held by a company that is not an issuing body. This is a company with which, since the initial approval to use the Kinegram machine, OTS has had no ongoing relationship and consequently had no ability to audit. At the time of approval,

[30] A Kinegram is a proprietary product which uses a security foil and film to safeguard documents against forgery and falsification.

there was no risk assessment undertaken by OTS related to the company. Following the approval of this card printer in 2006, OTS did conduct an inspection of the facilities and was satisfied with the security arrangements. However, there has been no subsequent oversight by OTS. This company has produced over 35 000 current security identification cards.

Verification of cards

3.19 The risk of false cards being produced and used is an inherent risk associated with any identity card scheme. Having a large number of issuing bodies, as in the case of the ASIC and MSIC schemes, places particular emphasis on the management of this inherent risk.

3.20 In practice, the risk of false cards is not currently tested in a substantive way. However, OTS does hold data that could provide some insight in this regard. From time to time, OTS officers in the field record details of an individual's ASIC or MSIC. OTS, however, has not to date used this information to conduct any confidence checking or assurance that the cards were in fact legitimate.

3.21 The ANAO sought to match the ASICs and MSICs details collected by OTS officers against the AusCheck database, using a range of methodologies, including fuzzy searching. From a total of 55 cards, there were 53 corresponding records in the AusCheck databases—in two cases no corresponding record in the AusCheck could be found for the cards recorded. Further work by OTS identified that one card was initially issued by one issuing body; however, following a revocation of the particular issuing body, the details of the cardholder were not appropriately transferred and maintained. The second card the ANAO identified was issued without an AusCheck background check, most likely due to an administrative error. Following identification of the card, the issuing body advised OTS that the card had been returned and the individual had been issued with a new security identification card based on a clear background check. The issuing body further advised that they had enhanced procedures for their processing of cards.

3.22 While the sample cannot be seen as representative of the total population, the fact that even with this small sample it was possible to identify ASICs and MSICs that had been printed and had no correlating record in the AusCheck database, suggests that this is a matter requiring further management attention.

Confirming an applicant's identity

3.23 All issuing bodies have the responsibility to confirm an applicant's identity. There are a range of documents that can be accepted by issuing bodies based on a primary, secondary and tertiary classification of documents.[31] Confirming the correct identity of an applicant is integral to the background checks, which are conducted based on the information submitted by the applicant. It is important that issuing bodies retain evidence of identity confirmation to provide assurance that these requirements are being met.

3.24 OTS compliance and audit activity includes a limited review of issuing body compliance with these requirements. For example, the ANAO observed that some of the audits conducted included a review of five recent applications and confirmation that the correct documents had been retained. The ANAO also undertook analysis using a sample of all cards issued by two issuing bodies. Each issuing body reviewed by the ANAO had missing records relating to the confirmation of the identity of the applicant. One issuing body was only able to produce the required documentation for 29 of the 40 applicants of the sample (75 per cent), while the other issuing body was able to produce documentation for 12 of the 21 applicants of the sample (57 per cent). While these examples are only from two issuing bodies, it indicates that more compliance activity may be required to gain assurance that identification requirements are being fulfilled.

Conclusion

3.25 Overall, the application process for ASICs and MSICs involves many parties and different processes. Under the schemes, some of the critical elements, including card production, have been outsourced to companies outside the direct purview of OTS. While the schemes prescribe mandatory standards for issuing bodies, these standards are not being consistently met by some issuing bodies. Some administrative processes have also increased the risk of ASICs and MSICs being used inappropriately or intercepted for use by a person to whom the card was not issued. These risks have not been assessed or monitored by OTS in a systematic manner. There is scope to review the practices of issuing bodies and assess whether the current arrangements provide an appropriate level of assurance that the schemes' requirements are being met.

[31] See ATS Regulation 6.04 and MTOFS Regulation 6.07G.

Recommendation No.1

3.26 To strengthen the ASIC and MSIC schemes, the ANAO recommends that OTS:

(a) reviews the risks arising from the administrative practices of issuing bodies, particularly in the issuing and manufacture of cards, and evidence of the confirmation of an applicant's identity; and

(b) uses the outcomes of the review to assess whether the current arrangements provide an appropriate level of assurance that the schemes' requirements are being met.

DIT Response: *Agreed*

3.27 Appendix 1 sets out DIT's complete response to the recommendation.

Background checking

AusCheck responsibilities

3.28 AusCheck's role in background checking for ASICs and MSICs is to assess each applicant's details against the criteria and parameters established in the ATS and MTOFS Regulations, and make a final recommendation whether or not the statutory criteria have been met by the individual. This is achieved by: coordinating the applicant's background checks[32] with CrimTrac, ASIO and DIAC; making assessment decisions through the consistent interpretation of the statutory requirements and notifying issuing bodies of the outcome of those checks.

3.29 As part of the background checking process, AusCheck is also responsible for notifying applicants if, as a result of background checking, there is unfavourable criminal history advice and must give the applicant 28 days to submit additional information. AusCheck must also advise DIT if a security assessment of an applicant is adverse or qualified.

[32] 'Background check' under both the ATS and MTOFS Regulations means an assessment under the AusCheck scheme of information about any of the matters mentioned in section 5 of the AusCheck Act. 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 (as defined in subsection 35(1) of the *Australian Security Intelligence Organisation Act 1979*) 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) the identity of the individual.

Internal processes

3.30 AusCheck is required to meet a range of legislative requirements and performance targets. To support these objectives, AusCheck has developed an extensive range of Standard Operating Procedures (SOPs). These SOPs provide staff with instructions and procedures on how to do their work and follow the proper regulatory procedure. To further support the process, AusCheck uses a range of checklists and templates so that the correct legislative criteria are used and proper notification to applicants (or issuing bodies) is made. Combined, these various tools, along with the SOPs, provide AusCheck staff with a sound framework for efficient decision-making.

Criminal history assessments

3.31 The criminal history assessment involves the assessment of an applicant's criminal history as compared to the legislative schemes. The ANAO assessed AusCheck's performance of this task based on a sample of all applications processed on two random days within the sample period. A total of 88 criminal history background checks were assessed (60 ASIC and 28 MSIC). Assessors correctly applied the Aviation and Maritime-Security-Relevant Offence assessment criteria for all applicants who had a disclosable court outcome in the ANAO's sample.

3.32 The ANAO also assessed a sample of recent applicants with conditional or adverse assessments. A sample of 20 applications were analysed to assess AusCheck's compliance with key assessment procedural controls for processing applications including: adherence to their quality assurance processes; appropriately notifying applicants of their appeal rights; and notification of the ability to request a discretionary card from DIT. The ANAO found that in all cases AusCheck had complied with its SOPs and legislative requirements.

3.33 AusCheck is under certain obligations regarding the destruction of criminal history records received from CrimTrac.[33] Generally, this involves the destruction of criminal records following the AusCheck assessment. The ANAO identified four (from a reduced sample of ten) instances where the criminal history was retained on file beyond the agreed timeframe. The ANAO

[33] Broadly, AusCheck is obliged to destroy criminal history after: three months from date of receipt from CrimTrac: or six months from date of receipt from CrimTrac where the criminal history information has led the applicant being determined to be adverse or qualified against the ASIC or MSIC assessment criteria.

also identified a range of other instances during fieldwork where the criminal history was retained beyond the agreed timeframe. Following identification of these administrative oversights, AusCheck advised the ANAO that the criminal history records have been destroyed and its SOPs were revised to address this issue.

Mandatory information in the AusCheck database

3.34 In processing an ASIC or MSIC application, the issuing body provides a range of material (including personal information) to AusCheck. The AusCheck regulations mandate this information to include the name, a photograph of the applicant, the card number and the location where the card is valid.

3.35 Issuing bodies have been largely compliant with providing AusCheck with most of the required personal information, except for the requirement to provide photographs. AusCheck Regulations 14 (2)(b) gives AusCheck the authority to provide an exemption for issuing bodies from the need to supply a photograph. Initially, AusCheck used this clause to provide a grace period to active issuing bodies. Exemptions were granted for a period of 12 months and these have all expired. A number of issuing bodies sought extensions to the initial exemption; however, these have now all lapsed and all records on the AusCheck database, including those lodged when an exemption was in place, should have an attached photograph.

3.36 The failure on the part of issuing bodies to supply photographs has been an ongoing issue for AusCheck. AusCheck has sought to resolve this issue through the use of exemptions as well as by highlighting the responsibility of issuing bodies through papers delivered at working group meetings. It has also revised its process for uploading photographs in an attempt to make the process technically easier. These measures can be linked to improvements in photograph lodgement rates. For example, the percentage of AusCheck records with photographs increased from 45 per cent at June 2010 to over 80 per cent in January 2011.

3.37 The completeness of the AusCheck database is an important element of the ASIC and MSIC schemes. While there is no audit or penalty scheme associated with the AusCheck legislative framework, AusCheck does have the ability to not accept applications from non-compliant issuing bodies. Taking this step would require care and could substantially affect the ASIC and MSIC application processes. It is likely that the resolution of this issue will require

the involvement of both AusCheck and OTS to look at the process together to find workable solutions, as both agencies have a role to play in assisting issuing bodies to fulfil their obligations.

ASIC and MSIC processing performance

3.38 The AusCheck database automatically distributes requests for background checks to the background checking bodies, and approves any requests that do not have any aviation or maritime-security-relevant offences.

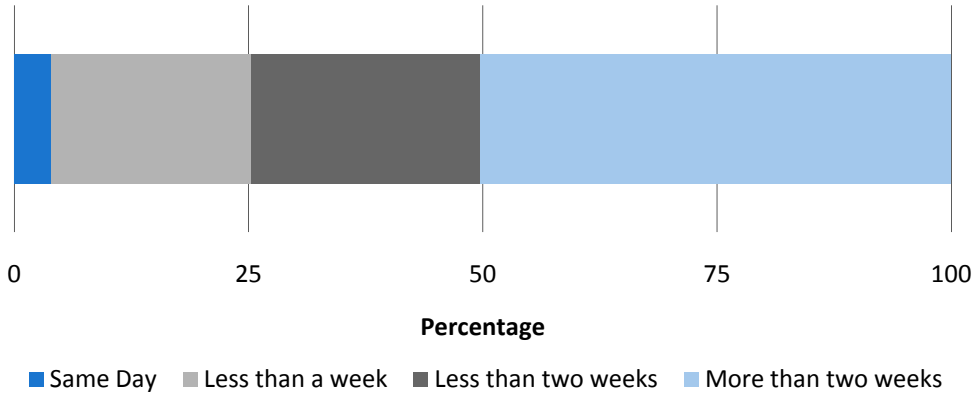
3.39 When AusCheck was established there was a key performance indicator (KPI) regarding timeliness which was: 'to provide timely and effective background checks for ASIC and MSIC issuing bodies'. While this KPI has been removed, there is an ongoing imperative for AusCheck to provide timely background checks, which is included in AusCheck's service charter. The current internal service standard is that AusCheck will complete its part in the background checking process in five business days or less, 98 per cent of the time.

3.40 The ANAO assessed the time taken to process ASICs and MSICs by AusCheck, based on an extract of the AusCheck database in June 2010 of all current cards. The ANAO assessed two key time periods: the 'AusCheck processing time' and the 'end-to-end' processing time—the complete time taken from submission to completion.

3.41 The ANAO analysis shows that AusCheck processed 97 per cent of its background checking activity within one day and 99 per cent was completed in five business days or less. In terms of the 'end-to-end' processing time, around 50 per cent of checks were completed within two weeks. The total time of a background check may also be affected by the time an application is assessed by the background checking partners. Figure 3.2 details the end-to-end processing time.

Figure 3.2

End-to-end processing time of all current cards as at June 2010



Source: ANAO analysis.

Processes for the review of rejected applications

3.42 The ASIC and MSIC application process allows for a range of review mechanisms. An applicant can appeal AusCheck's decision to the Administrative Appeal Tribunal (AAT). However, in 2009–10 there were no finalised appeals to the AAT.[34] Alternatively, an applicant can accept that there is no error of fact made by AusCheck, but can apply for a discretionary ASIC or MSIC and provide additional information that demonstrates that the person is unlikely to be a threat to aviation or maritime security—this occurred 112 times in 2009–10.

3.43 Broadly, OTS administers two discretionary ASIC and MSIC processes. The first process allows the Secretary of DIT to issue a discretionary card for applicants who have been found to have an adverse criminal history. People who have been refused an ASIC or MSIC may apply to the Secretary of DIT for a discretionary card either directly or through their issuing body. The second process broadly provides for MSIC applicants who may have their original

[34] One AAT appeal was notified to AusCheck on 29 June 2010. It is ongoing and is before the AAT. Six AAT appeals were settled in 2009–2010 without going to final hearing. Of those, five were withdrawn and one was settled by the Commonwealth entering into consent orders, and two other appeals were commenced but were withdrawn.

application to the Secretary for special circumstances reconsidered under MTOFS Regulations.[35]

3.44 To support the processing of discretionary ASICs and MSICs, OTS has developed 'how to' guides. These documents cover the various stages of the application process and the department's obligations. The guides also include templates and checklists to assist staff. Taken together, OTS's administrative processes and 'how to' guides provide an appropriate framework for supporting the assessment of discretionary ASIC and MSIC applications.

3.45 To assess OTS compliance with these processes, the ANAO reviewed a sample of 21 applications for a discretionary ASIC or MSIC from 2009–10. OTS adhered to internal procedures for the ANAO's sample. This included consideration of the additional criteria under the ATS and MTOFS Regulations regarding the nature of the offence and the length of the term of imprisonment imposed. OTS also prepared a statement of reasons for all 17 cases reviewed where one was required and applied a risk-based, evidence-informed approach to assess whether the applicant represented a risk to transport security. The ANAO did identify, however, seven examples where applicants had not been advised of their appeal rights and two cases of the appeal not being processed in the statutory mandated 30 days. OTS advised the ANAO it has revised its processes to remedy these issues.

3.46 The process of discretionary ASICs and MSICs allows the Secretary of DIT to issue cards with conditions. The most common condition is a restriction on the validity period of the card. The ANAO notes, however, that the discretionary card process creates an anomaly in the ASIC process. Under the ATS Regulations, individuals with a qualified criminal record are eligible for an ASIC with 12 month validity; however individuals with an adverse criminal record are ineligible for an ASIC.[36] Through the discretionary ASIC process, an individual with what in some cases could be the more serious adverse criminal record may receive a two-year ASIC depending on the full range of

[35] This application is made under MTOFS Regulation 6.08X. There are a range of circumstances that an applicant can apply under this regulation including if the background check of an applicant reveals that he or she has been convicted of a disqualifying offence; or the security assessment of the person is adverse and is not a qualified security assessment.

[36] The difference between a 'qualified' and 'adverse' criminal record is described in detail in Appendix 2. Broadly, subject to timing criteria, if an individual has been convicted of an aviation-security-relevant offence and sentenced to imprisonment the individual has an *adverse criminal history*. If an individual has been convicted twice or more of an aviation-security-relevant offence and did not receive a sentence for imprisonment, the individual has a *qualified criminal record*.

circumstances of the case. While ANAO has not identified cases where this has led to a significant injustice, it is a potential inconsistency in the ASIC scheme.

3.47 In 2009–10, 100 per cent of completed discretionary ASIC applicants (70) were approved with either a 12-month or two-year ASIC. A further three applications were withdrawn part way through the process. In relation to discretionary MSIC applications, in 2009–10, 97 per cent (35/36) of completed discretionary MSIC applicants were approved with either a 12-month, three-year or five-year MSIC. A further two applications were withdrawn part way through the process.[37]

[37] The ANAO notes an applicant has an appeal right for a review of OTS' decision regarding discretionary cards to the AAT.

4. Information Management

This chapter examines the information technology (IT) environment supporting the AusCheck database as well the integrity and the accuracy of ASIC and MSIC data holdings.

Introduction

4.1 AusCheck, in processing and maintaining a central register of all ASICs and MSICs, relies on one main information technology (IT) system. The reliance on a single database emphasises the importance of AusCheck establishing practices and assurance processes regarding the integrity and accuracy of information. A lack of appropriate processes could result in ineligible persons receiving ASICs and MSICs or significant delays and costs to the industry.

4.2 The ANAO reviewed the IT environment supporting the AusCheck database. While AusCheck has overall responsibility for the database, database support and maintenance services are provided by the Attorney-General's Department (AGD). Given this outsourcing arrangement, the specific areas of focus were AGD's IT governance and system support processes as well as the integrity of the AusCheck database itself.[38]

4.3 The ANAO also worked closely with 11 issuing bodies to assess the accuracy and integrity of their ASIC and MSIC data holdings. This work covered over 50 per cent of the total ASIC and MSIC population.

Overview of the IT environment

Governance arrangements

4.4 The IT governance arrangements between AGD and AusCheck use a simple command structure that is centred on an AusCheck IT Project Board. AusCheck's IT needs are communicated in this forum and are used to inform AGD's IT strategy and activities. The Project Board monitors the progress of IT activities and manages the impact on AusCheck's business. The delivery of IT

[38] The audit applied selected processes from Control Objectives for Information and Related Technology (CobiT), a framework of internationally accepted standards, to assist with assessment of key aspects of AGD's management and operation of IT. The audit also relied on elements of the Information Technology Infrastructure Library (ITIL) framework.

needs is managed through the AGD project and change management processes and is appropriate for AusCheck's business needs.

4.5 AGD has a risk management framework and IT risk is managed by the IT division. The IT risk assessments include broad technological and information risks, and the respective mitigation strategies. These risks are not specifically focused on single systems, such as AusCheck, but the overall set of IT risks that affect AGD operations. AusCheck IT risks, specifically those relating to security and continuity, are assessed as part of the system accreditation and business continuity processes. The ANAO considers that this level of focus is appropriate for AusCheck's business.

4.6 AGD has established a security management framework, including the definition of policies, plans and procedures. In line with AGD's ICT Security Policy, systems must be accredited prior to being placed into the production environment. While mainly an administrative oversight, the accreditation process occurred in March 2011. There is also a current System Security Plan that provides an overview of the security requirements of the AusCheck's system.

4.7 User access to the AusCheck database is controlled through formalised processes and access to privileged or administrator functions are restricted. AusCheck database users are required to authenticate their identities through usernames and passwords; and access to AusCheck database functions, such as the approval of security checks, is controlled through user profiles. A limited number of AusCheck staff have access to privileged or administrator database functions. An inherent difficulty with the access controls is that AusCheck has little oversight of the policy and procedures of the issuing bodies that are accessing the database.

4.8 The first operational AusCheck database was completed in September 2007. This was developed following two failed attempts that did not provide the agreed system functions and had several security issues. At the time of these developments, AGD did not have a formalised Project Management Framework. The department has since implemented a framework based on the PRINCE2 (Projects in Controlled Environments 2) methodology, which is widely used in both the public and private sectors. This process is facilitated by a Project Office that supports communication between the steering committees, project boards and project teams.

4.9 In June 2010 AusCheck and AGD agreed to a service level agreement designed to 'ensure that the proper elements and commitment are in place to provide consistent IT service support and delivery to AusCheck.' The agreement includes the charging model, service scope and responsibilities, and service management requirements.

4.10 AGD has established an IT governance framework to support not only AusCheck's business but the overall operation of AGD. AGD's IT governance framework provides adequate structures and processes to sustain and extend AusCheck's business requirements.

System support processes

4.11 AGD has implemented several processes to assist with the ongoing operation and availability of the AusCheck database. These support processes include:

- basic monitoring of operational logs;
- a largely reactive problem management program; and
- the development of a service level agreement in July 2010 establishing agreed standards and performance targets.

4.12 These support processes help manage changes and access to the AusCheck database, and are focused on monitoring and resolving AusCheck database problems. These processes have largely been successful as there have been no major problems or outages. Going forward, and depending on available resources and assessment of relative priorities, the current support processes would be enhanced by more sophisticated monitoring of operational logs, and a problem management program that focuses on prevention.

Integrity of information

4.13 Complete, accurate and current information is critical to making good decisions. AusCheck has established a number of controls over data input, including:

- mandatory data requirements, which include data field validation on data entry forms, such as date validation and validity of post codes;
- security checking to determine proper access authorisation to AusCheck database data;

- audit logging, such as user logon, general exceptions and system availability;
- business rules that are defined to check data entry, existence of data and satisfaction of pre and post conditions before recording the entry in the AusCheck database; and
- data constraints, such as mandatory, data type requirements and dependencies with other data (for example a security card cannot exist without being associated with an issuing body).

4.14 An inherent risk with the AusCheck database is the reliance on issuing bodies to update data; this affects the currency of all the data in the database. While AusCheck has implemented mandatory data requirements, there is no direct link between the AusCheck database and the issuing body's data holdings and no ongoing control to align these two data sets. While there are inherent risks in the currency of the AusCheck data, the database has adequate controls to reduce the risk of errors relating to completeness of information. These include mandatory data requirements, standard reports and exception handling processes.

Legislative and business requirements

4.15 The ANAO also assessed a range of legislative and business requirements, including whether:

- all ASICs and MSICs are associated with a registration, individual and issuing body;
- all individuals over the age of 18 have undergone a security check prior to receipt of an ASIC or MSIC;
- any ASIC or MSIC with convictions were reviewed; and
- each ASIC and MSIC had an expiry date within the defined AusCheck period.

4.16 The ANAO found that the data aligned to the majority of the requirements selected. The ANAO identified seven expired cards that did not have an expiry date nor had valid AusCheck periods (that is, no start and end dates, or the end date was greater than the start date) specified. These were largely due to the card details not being automatically updated when replacement cards were issued (the required manual updates had not been performed). The examples of data errors however, were insignificant in the

total population of the AusCheck database. The database controls regarding the legislative and business requirements were reasonably sound.

Accuracy of ASIC and MSIC data holdings

4.17 While AusCheck maintains a database of all applications it has processed, each issuing body is also required to maintain a database of all cardholders. In theory, there should be alignment between the different databases of current cardholders. The ANAO examined the accuracy of the ASIC and MSIC data holdings by comparing the records held by AusCheck with the records held by each issuing body.

4.18 In analysing the comparative records, it was important to understand how a record of a decision is created on the AusCheck database. The establishment of a record in the AusCheck database occurs instantly following advice to issuing bodies that the applicant had satisfied the background check. Although the decision to actually issue the card rests with issuing bodies, the AusCheck database identifies that the card is issued following a successful background check. While issuing bodies are required to notify AusCheck if they decide not to issue the security identification card, this arrangement makes an assumption that all individuals who satisfy the background check are issued cards, and that this process occurs instantaneously.

4.19 Issuing bodies, as part of their reporting obligations, are required to advise DIT at the end of the financial year on a number of specific activities. While these obligations vary slightly between the ATS and MTOFS Regulations, both schemes require issuing bodies to provide aggregate statistics on the total number of current cards. To support issuing bodies in fulfilling their obligations, OTS facilitates the annual reporting requirements by initiating the contact and following up non-responses. However, OTS does not always receive survey responses from every issuing body, and some issuing bodies fail to answer some non-mandatory questions that are asked by OTS.

4.20 The ANAO compared the results of the reported data with AusCheck data from a selected sample of issuing bodies. The issuing bodies selected in the sample account for over 50 per cent of all cards issued, and covered third party issuing bodies, airlines, airports and government issuing bodies. There were significant variances. The ANAO conducted further work with the sample issuing bodies to gain a better understanding of the variances. This

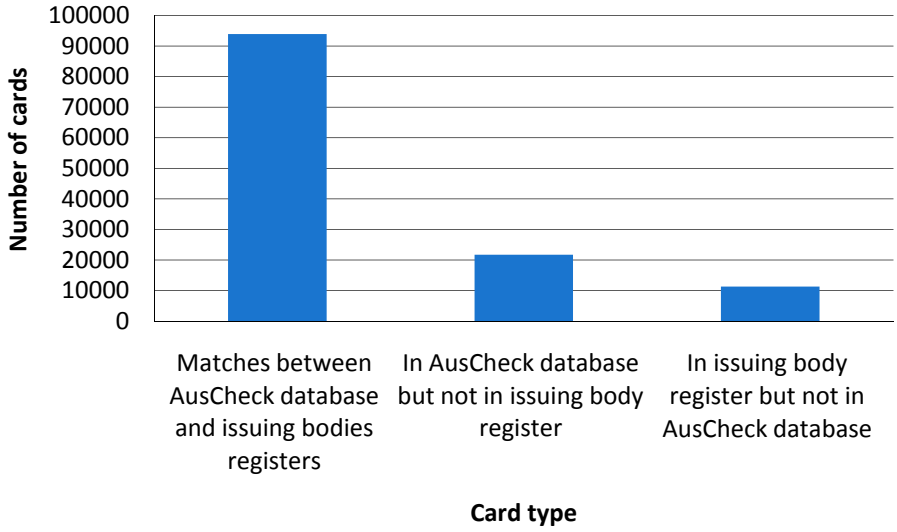
involved data matching the records of the issuing body with AusCheck data. From this process, three distinct populations emerged:

- exact matches between AusCheck and the issuing body;
- cards registered on AusCheck but not in the issuing body register; and
- cards registered in the issuing body register but not in AusCheck.

4.21 Figure 4.1 provides a summary of the total figures within each of the populations.

Figure 4.1

Number of cards from selected issuing bodies matched against the AusCheck database



Source: ANAO analysis of AusCheck and issuing body data.

4.22 The ANAO provided each issuing body with a sample of card details from each population. AusCheck was also provided with details of the variances. Issuing bodies and AusCheck provided the ANAO with a range of explanations regarding the variances between the data matching results. The ANAO notes that through this process, these variances were largely due to

administrative or process differences and errors.[39] Table 4.1 lists some of the cited explanations.

Table 4.1

Explanations of the variances between the AusCheck database and issuing bodies' registers

Cards in AusCheck database but not in issuing body register
Issuing body not updating AusCheck database to reflect cancelled and destroyed cards
Timing difference between when a card is marked as issued by AusCheck and the actual issue of the card by the issuing body
Errors in how issuing bodies respond to reporting requirements
Cards in issuing body register but not in AusCheck database
Issuing body not updating AusCheck database to ensure correct card number is recorded (especially for renewals)
AusCheck migration issues (largely relating to older MSIC cards)
Under 18s who do not have to be registered with AusCheck
MSICs issued under the provision whereby the issuing body can issue an MSIC if an ASIC has been already issued, however AusCheck was not notified
Cards that had been cancelled in AusCheck by the issuing body, but reactivated by issuing body, but AusCheck was not notified

Source: ANAO analysis of AusCheck and issuing body responses.

4.23 The ANAO further notes that some issuing bodies were incorrectly responding to their annual reporting requirements. For example, one issuing body was providing details of all cards issued in a financial year, whereas the requirement is to provide the total of all current cards, an error repeated in the last three years of reports. While OTS has collated the data provided by issuing bodies, the data has not been subject to any quality assessment for accuracy. It is likely that such an assessment of the reported data would have noticed the issues the ANAO has identified. The ANAO suggests that OTS reviews the annual reports to identify any errors in reporting and reminds the issuing bodies of their obligations.

[39] The ANAO notes that there were changes made to the ASIC and MSIC schemes on 1 December 2010 following the ASIC enhancement project and the MSIC review—see Chapter 2. Part of these changes included penalties that may be imposed on issuing bodies that fail to comply with particular aspects of regulations, including updating the AusCheck database. These new provisions may assist in getting closer alignment between the AusCheck database and issuing bodies' registers.

4.24 The accuracy of an issuing body's database and its alignment to the AusCheck database is important to gain assurance about the integrity of all current ASICs and MSICs. The AusCheck database was established to provide a 'comprehensive database of all applicants and ASIC and MSIC cardholders.'[40] However, a consequence of having multiple responsible issuing bodies with varied processes reduces the assurance around the total number of current cards, or the currency of all cards on the AusCheck database. Currently, OTS conducts basic checks of issuing bodies' compliance with the regulations but does not assess the processes or systems of issuing bodies in a systematic way (discussed in Chapter 5). OTS has the ability, through more focused compliance activity, to gain further assurance around the procedures and practices adopted by issuing bodies as well as the accuracy of the various databases.

[40] Second Reading Speech, *AusCheck Bill 2006*, House of Representatives Hansard, 7 December 2006, p. 12.

5. Compliance Activities

This chapter examines the development and implementation of the compliance framework for ASICs and MSICs including the enforcement regime and cardholder obligations. The visitor identification scheme is also discussed.

Introduction

5.1 OTS's regulatory philosophy articulates the approach and manner used to seek voluntary compliance by industry participants. OTS identifies its role as to 'provide expert advice and regulatory oversight for the Australian Government by taking a risk-based approach that continuously enhances security in Australia's transport sector'.[41] OTS's approach to regulation is to assist industry compliance with the law and regulations by effecting changes in industry participant behaviour towards their regulatory obligations. OTS states that its strategies to deal with these participants range from educational activities through to prosecution.

5.2 The ANAO reviewed OTS's: compliance framework; enforcement regime; and visitor identification cards (VICs). Specifically, the ANAO assessed the compliance activities relating to all issuing bodies, as well as a sample of the compliance activities for 46 'high-risk' industry participants in 2009–10. Fieldwork was conducted across seven state and territories at 29 separate security controlled areas (including both security controlled airports and security regulated ports).

Compliance framework

5.3 The security arrangements for Australian aviation and maritime environments place responsibility on every industry participant to comply with relevant security plans. As noted in Chapter 1, there are currently over 1200 industry participants. This system has the inherent risk of industry participants not appropriately complying with their responsibilities. OTS manages these risks through compliance and education activities. It conducts a range of compliance activities across the aviation and maritime industries to assess compliance with Australia's transport security legislation and the

[41] Commonwealth of Australia, *Office of Transport Security Strategic Plan 2007–2010*, 2008.

security plans of industry participants. The compliance activities include regulatory audits, inspections and security tests.

Compliance program

5.4 OTS releases its National Compliance Plan (NCP) annually. The NCP is based on identified key risks and outlines the mitigation strategies to be adopted. Central to the NCP is the process of segmentation and the development of 'heat maps' to guide the program of activity. Segmentation allows OTS to develop varying compliance strategies for different risk profiles, at both the industry level and sub-levels. The heat map process is designed to apply a systematic and disciplined approach to compliance risk management, where segments are rated with an inherent risk, a mitigation rating, and compliance priority.

5.5 OTS's regional offices are responsible for delivering the planned mitigation strategies,[42]which include audits, inspection tests and observations, relationship management and incident response management. The major focus of the mitigation strategy is audit activity.

Compliance manual and templates

5.6 OTS has a National Compliance Manual (NCM) to help conduct its compliance activities. The NCM assumes the compliance approach to each industry segment will maintain or improve levels of compliance within the industry.

5.7 The NCM is supported by a suite of templates and tools that OTS staff use in their activities. These compliance templates are an effective way of ensuring key elements of the scheme are assessed in each audit or inspection. While the ASIC and MSIC schemes are only one aspect of the overall OTS compliance scheme, elements of ASIC and MSIC schemes (in particular card display) are incorporated in 35 of the 49 compliance templates. The ANAO observed that the range of templates used by OTS, until 2010, varied between the different regions. While the substantive elements of the templates covered the same topics, the audit approaches varied between each region. A consequence of this was that companies that operated across state boundaries would be subject to different approaches depending on the location of their

[42] OTS has divided their activities between five regional offices—NSW/ACT, Queensland, Western Australia, Victoria/Tasmania, South Australia/Northern Territory.

activities. In 2010, OTS was in the process of standardising and implementing a the whole suite of templates aimed at resolving this issue. During fieldwork, the ANAO found examples of the new templates being used.

5.8 OTS also has a detailed ASIC and MSIC audit template that is used for audits of issuing bodies and covers compliance with key sections of the legislative scheme. Like other compliance templates, the ANAO observed that while the format of the template differed between regions, the content was consistent. At times OTS did not use the ASIC issuing body audit template, but assessed broadly how ASICs are issued and managed by issuing bodies as part of the annual airport security audits. These audits were less extensive than the specific issuing body audits and generally covered the ASIC registers as well as a general discussion about their application and issuing procedures (approximately five or six questions within the audit tool). Similar to the specific issuing body audit tools, the format of the template for annual airport security audits differed between regions. However, the content was consistent.

Compliance activity

5.9 Compliance audits are usually conducted once a year on high-risk industry participants, with supplementary audits scheduled as necessary to gain assurance that industry participants have implemented corrective action plans arising from the annual audit. OTS also conducts a schedule of routine inspections, as well as targeted inspections in response to identified incidents of non-compliance. These inspections are conducted in accordance with the NCM.

5.10 The ANAO reviewed both the general compliance activity of OTS and the audit activity conducted on particular issuing bodies in 2009–10. A sample of 46 industry participants was assessed. While the 46 industry participants were from different market segments across Australia (including airlines, aviation and maritime) the ANAO assessed the same high-risk categories from different regions to enable comparative analysis.

5.11 The ANAO found that the approach to compliance activity differed across the different regions due to historically different templates as well as the proximity of the regional offices to key aviation and maritime sites. Notwithstanding the differing approaches, all regions assessed compliance with the core regulations as part of their compliance activities.

5.12 The ANAO review identified a number of examples where compliance activities could be improved. From the sample of 46 compliance files there was:

- an example of a critical issue identified in an annual audit not yet followed up in subsequent audits;
- six examples of failure to follow procedures in audit sign-off;
- inadequate audit documentation in one case; and
- differences in how non-compliance is reported; for example, some regions report non-display of an ASIC or MSIC as a non-compliance for internal reporting, whereas other regions take a more informal approach.

5.13 The ANAO also specifically assessed OTS' audits of issuing bodies. Given the varied profile of ASIC and MSIC issuing bodies, these audits, as previously noted, are conducted as either standalone audits or as part of the annual security audit. The top ten issuing bodies (by volume of current cards) that make up 89 per cent of the MSIC market have all been audited by OTS during the 2009–10 financial year as standalone audits. OTS also audited ASIC issuing bodies, generally as part of the airport annual audit. The ANAO considers OTS compliance activity surrounding issuing bodies is appropriately focused on the higher risk issuing body (with consideration of size and proximity to potential targets).

5.14 OTS compliance activities surrounding industry participants, as well as ASIC and MSIC issuing bodies, cover basic compliance with the regulations and either security plans or issuing body plans. However, a large component of the checklists covers processes that would not necessarily change from year to year, such as the existence of a register, annual reporting procedures, the form of the card, and procedures for issuing cards. By contrast, the compliance tools do not explicitly cover more dynamic actions taken by the industry participants or issuing bodies, such as actions to continuously improve processes, nor do the tools assess how the entity has implemented findings from internal audits or review findings. While OTS uses formal observations as a way of alerting industry to potential security vulnerabilities, further refinement of the compliance tools would lift the focus towards management improvements and enable more effective management assurance about industry and issuing body compliance with requirements.

5.15 The regime could also be strengthened if information obtained through OTS's audit, inspection and stakeholder programs was better used to inform and target compliance activities. For example, greater use of past audit and compliance activity could focus the compliance activities in areas that represent the greatest security risk—areas where previous examples of non-compliance have been identified.

5.16 As part of the compliance assurance framework, OTS has developed a Quality Management System (QMS), which includes a quality assurance program. The QMS is designed to be a programmed approach to the review of business processes and outputs, to identify areas of better practice, systemic problems and probable causal factors. At the time of the audit, OTS was in the initial stages of rolling out the quality assurance program. As a consequence the ANAO was unable to assess the contribution the QMS has made to OTS's compliance activities. The ANAO notes, however, that the QMS should provide OTS with an important mechanism to assess its own performance and enable it to focus on continuous improvement.

Cardholder obligations

5.17 ASIC and MSIC cardholders have obligations under the legislative scheme.[43] The ANAO observed a range of methods used by issuing bodies to notify and remind cardholders of their obligations. Common approaches observed during audit fieldwork included incorporating advice about cardholder obligations, in both paper-based and online applications. Some issuing bodies require cardholders to sign a form when they collect their ASIC and MSIC to acknowledge both receipt of the card and that they understand their responsibilities. The ANAO observed that some issuing bodies also require a bond or deposit, in addition to the card fee, for the ASIC or MSIC.

5.18 One of the most common audit findings by OTS is the non-display of an ASIC or MSIC. The ANAO also observed at various locations examples of individuals not wearing their cards.[44] While isolated instances of non-display is

[43] For example, ATS Regulation 3.03 (1) and MTOFS Regulation 6.07J requires individuals to properly display their ASICs or MSICs in aviation or maritime security zones respectively. ATS Regulation 6.45 and MTOFS Regulation 6.08P requires the return of ASICs and MSICs to an issuing body after: the card has expired, the card is cancelled, or the card is damaged.

[44] For example, on one occasion the ANAO observed OTS staff speaking to some cardholders about improper display of their MSICs. Despite the overt presence of OTS inspectors, a nearby group of individuals were also not displaying their cards. The cards were only displayed after OTS inspectors spoke directly to the individuals.

an ongoing issue, the ANAO observed general compliance during site visits to 29 different security controlled areas across seven states/territories in Australia. The ANAO notes some of the ongoing issues of non-compliance may, in part, be addressed by the proposed pilot trial of the Security Infringement Notice system (discussed in paragraph 5.29).

5.19 In addition to non-display there are also issues associated with the return of cancelled or expired cards. The 2004 JCPAA Report 400—*Review of Aviation Security in Australia* raised a specific concern with the non-return of expired cards. Cardholders are responsible for returning cancelled or expired cards to the issuing body and failure to return the card is a strict liability offence. While in theory a cancelled or expired card can no longer be used, cards can also be embedded with access control that might not expire at the same time as the card. Furthermore, the ANAO observed that, when used for access purposes, security guards often had little opportunity to confirm the currency of the cards. As a consequence, the return of cancelled or expired cards is an important control in ensuring only current cards are being used.

5.20 The non-return of expired and cancelled cards has been an ongoing issue for many years. The evidence suggests that the current method of educating cardholders of their obligations has not been fully effective. For example, OTS receives some data on non-return rates through annual reporting by issuing bodies. The ANAO's analysis of the 2009–10 reports indicate that:

- in the ASIC scheme, 12 100 from a population of 40 652 (30 per cent) cancelled or expired cards in 2009–10 were not returned to the issuing body; and
- in the MSIC scheme 601 from a population of 2 225 (27 per cent) cancelled or expired cards were not returned to the issuing body.

5.21 The reports also show that some issuing bodies have achieved relatively high return rates, compared to other issuing bodies. OTS compliance activities include a specific focus on issuing bodies returning cancelled or expired cards as well as the procedures for the return of cards. However, the effectiveness of the different processes used by issuing bodies for card return is currently not assessed in a systematic way by OTS. The data collected by OTS through the annual reporting obligations could be used to assist issuing bodies in the identification of better practice.

Conclusion

5.22 OTS has established a compliance framework for the ASIC and MSIC schemes that is aimed at ensuring industry participants and issuing bodies meet legislative and regulatory requirements. While a newly developed QMS should provide an increased focus on continuous improvement, there is scope for OTS to increase its use of information obtained from its audit, inspection and stakeholder programs to focus its future compliance activities.

Recommendation No.2

5.23 To provide increased assurance and improve the outcomes of its compliance activities, the ANAO recommends that OTS:

(a) increases its use of information obtained from its audit, inspection and stakeholder programs to focus future compliance activities on areas that represent the greatest security risk; and

(b) captures and shares elements of better practice identified through their compliance activity with industry participants.

DIT Response: *Agreed*

5.24 Appendix 1 sets out DIT's complete response to the recommendation.

Enforcement regime

5.25 In addition to audit activities, the ATS Act and MTOFS Act provide an enforcement regime for non-compliance. Under both Acts, provisions exist for criminal offences but to provide flexibility a range of enforcement options can be used as an alternative to, or in addition to, criminal prosecution. These include infringement notices, enforcement orders, ship enforcement orders (maritime only), injunctions and a demerit points system. Many of the offences are based on a strict liability scheme that can be enforced by authorised persons including law enforcement officers or a Transport Security Inspector (TSI).[45]

5.26 The enforcement regime is an important element of OTS's regulatory philosophy. Possible actions in response to any instances of non-compliance potentially include infringements and enforcement orders. Within the ASIC

[45] Transport security inspector includes both aviation and maritime security inspectors. Within the ATS Regulations an airport security guard is also an authorised person.

and MSIC context there are a range of potential penalties directed at individuals, industry participants and issuing bodies including:

- improper display of a valid ASIC and MSIC—five penalty units;
- non-supervision of a person who has a VIC—five penalty units;
- improper form and design of the ASIC and MSIC cards—50 penalty units;
- issuing bodies not giving effect to its issuing plan—50 penalty units; and
- industry participants not ensuring that access to a security restricted area can only be accessed by the appropriate people—200 penalty units.[46]

5.27 As at March 2010, OTS had not formally used any of the enforcement powers under the ATS or MTOFS Regulations. However, a small number of charges had been laid by state police under the MTOFS Regulations.

5.28 Increased enforcement activity is an aspect that some industry participants are keen to see improved. For example, the incorrect display of an ASIC or MSIC is a common finding of OTS compliance activities. While industry response to non-display includes induction programs, education and additional signage, the ANAO was advised there is also support for a greater role for OTS. This advice came from a range of industry participants across Australia. In correspondence to OTS, one industry participant advised OTS that they believe '...the only effective measure to address this matter is for the OTS to issue individual fines to those who fail to observe the regulations.' At the time of ANAO fieldwork, OTS was yet to provide a direct response to this suggestion.

5.29 In 2010, OTS's Policy and Audit Committee endorsed a pilot trial of a Security Infringement Notice (SIN) system. In the development of the SIN system, OTS noted 'the increased security fatigue and push back from industry' and the need for OTS to develop its capability 'to generate compliance and meet its strategic objectives.' The objective of the pilot is to trial the infringement provisions contained within the legislative scheme for a three-month period. The pilot was originally planned to occur in late 2010,

[46] As defined by the *Crimes Act 1914* (s4AA), a penalty unit is $110 at as November 2010.

however as at February 2011, OTS advised the ANAO that the pilot is still being planned with no specific date set. The trial's scope includes the issuing of formal caution and security infringement notices for specified offences as well as an evaluation to assess the success of the trial. The trial is planned at two locations in Australia in partnership with other Australian Government agencies.

5.30 OTS's regulatory philosophy states that possible compliance responses to non-compliance include prosecution. The underlying theory to this responsive regulation model is that prosecution not only has a direct effect on the industry participants concerned, but also has a significant deterrent effect on others. However, it regularly identifies examples of non-compliance, such as the improper display of ASICs and MSICs as well the lack of supervision of VIC holders, suggesting that education activities have not been fully effective.[47]

5.31 While OTS has a range of responses to cooperatively encourage compliance, there is a significant gap in its current approach to dealing with non-compliance. Although the ATS Act and MTOFS Act provide for an enforcement regime for non-compliance that includes a range of options that can be used as an alternative to, or in addition to, criminal prosecution, these powers have not been used. Emphasis has been placed on education activities only. OTS is developing an enforcement capability which, if effectively implemented, will assist it to deliver a graduated range of responses to address non-compliance.

Visitor identification cards (VICs)

5.32 The VIC scheme is limited to the aviation sector and allows issuing bodies or agents to issue a VIC to a person without a background check, if the person needs to enter the secure area of a security controlled airport and provided that the person will be supervised.[48] There are a variety of circumstances when a VIC may be issued. For example, the ANAO observed the issue of VICs to:

- contactors who were working on extensions to airports;
- new staff employed at an airport who were under probation; and

[47] During fieldwork, the ANAO also observed instances of non-display of ASICs and MSICs, as well as the lack of supervision of a VIC holder.

[48] ATS Regulation 6.38.

- the general contractor workforce involved in the ongoing maintenance of an airport (cleaners, rubbish truck drivers, and delivery vehicle drivers).

5.33 Under the regulations, unless otherwise agreed by OTS, the maximum validity period for a VIC is one month. However there is no limit to the number of VICs an individual may be issued. As such, it is possible for a person to move from one VIC to another for an indefinite period of time. While this does not present any legislative breaches, use of the VIC scheme in this way has the potential to undermine the broad intention of the ASIC scheme, whereby all persons regularly accessing secure parts of an airport are background checked.

5.34 The potential for the VIC to be used as means of bypassing the AusCheck process was identified in 2005 JCPAA Report 406—*Developments in Aviation Security since the Committee's June 2004 Report 400: Review of Aviation Security in Australia – An Interim Report*. In particular, the report recommended that the use of VICs should be restricted to exceptional circumstances rather than to facilitate ongoing access, as well as generally requiring all VICs to carry photographic identification of the cardholder. In response to JCPAA Report 406 and JCPAA Report 409 *Developments in Aviation Security Since the Committee's June 2004 Report 400: Review of Aviation Security in Australia*, in October 2008, the then Department of Infrastructure, Transport, Regional Development and Local Government advised the JCPAA that the department agreed that the provisions that regulate how VICs are issued should be tightened. As noted previously, in the Aviation White Paper issued in December 2009, the Government committed to a tightening of the provisions for visitor management at security controlled airports. To date though, there has been no change in these requirements, however, OTS advised that enhanced visitor management arrangements are close to finalisation.

VIC compliance

5.35 There is a range of obligations on industry participants and individuals relating to VICs. The ATS Regulations provide a formalised process for visitors including supervision, display requirements for cardholders and record keeping obligations for issuing bodies. For example, as part of the scheme VIC holders must be supervised at all times by an ASIC holder.

5.36 The VIC scheme also allows agents of issuing bodies to issue VICs on behalf of the issuing bodies. In a practical sense, a company leasing an

individual hanger at an airport may be an agent of the airport issuing body. The ANAO observed agents who had been given a number of cards with a log book as a means to record who has been issued a VIC and for how long. The ANAO noted that individual airports also manage agents in different ways. For example, at the time of fieldwork, at one gateway airport there were 46 agents whereas another gateway airport had none.

5.37 OTS compliance activities have identified a range of ongoing issues with VICs, including the role of agents. Examples of non-compliance found by OTS include:

- VIC registers of agents having missing fields and incomplete information;
- VIC agents who had a designated number of cards for VICs to be issued having missing cards;
- VICs being issued longer than the legislative allowed period;
- airport staff issuing VICs to themselves; and
- non-supervision of VIC holders—for example, workers signed in by agents at a hanger, away from the main terminal, who are left to undertake work unescorted.

5.38 The following case study highlights the vulnerabilities associated with unsupervised VIC holders having access to security zones.

Case Study

Many airports have a number of access gates for the delivery of goods and personnel associated with business at the airport. The access arrangements for each gate vary depending on the volume of traffic and security arrangements established within their Transport Security Plan (TSP).

At the airport visited by the ANAO there were contracted staff at the delivery gate. Following identification of the driver and passengers, the staff were required to conduct random cursory visual vehicle inspections. The TSP states 'As a general rule however, a third of the traffic entering the security restricted area (SRA) should be inspected. This consists of: visual inspection of the vehicle, internal inspection through the windows and inspection of the boot area/load.' ANAO observations of this gate were consistent with this aspect of the TSP.

Drivers without ASICs at this gate were provided with VICs, required to surrender photo identification, subject to the random cursory visual vehicle inspections and required to wait within the SRA under closed circuit television for an escort vehicle. The ANAO followed a VIC holder in a large truck who was waiting for an escort vehicle. The escort vehicle proceeded to the desired destination where it left the truck unsupervised. The truck and VIC holder remained unsupervised for over 30 minutes at this location. The ANAO did not observe on this occasion whether or not the truck had been inspected. Similar incidences have been noted at this access gate previously by the airport operator.

OTS subsequently advised the responsible parties involved in this incident of their compliance failure. OTS received a reply indicating that corrective action had been taken, including counselling and a memo issued to all staff about proper procedures.

VIC legislative changes

5.39 In December 2009, the Government announced in the Aviation White Paper that it would strengthen visitor arrangements. To give effect to the changes announced, OTS planned to progress the implementation of the enhancements outlined in the Aviation White Paper.

5.40 As previously noted in Chapter 2, DIT sought agreement from the then Minister for Infrastructure, Transport, Regional Development and Local Government in June 2010 to a number of changes relating to the VIC scheme due to come into effect by 1 December 2010. Following the election in 2010 and industry feedback, a new proposal was agreed to by the new Minister for Infrastructure and Transport in February 2011. The proposed changes seek to limit the aggregate number of days that VICs can be issued to an individual at a specific airport in a 12 month period, with full implementation planned to take effect in late 2011.

5.41 The proposed changes were extensively discussed with industry, which has been, in part, the reason for the long lead time between the original identification of the risk and the subsequent proposed treatment. A common

concern was the cost and practical implications of instituting some of the proposed changes.

5.42 In the process of industry consultation OTS received a wide range of perspectives and anecdotal evidence to support these perspectives. This process identified strong and divergent views held among participants in the aviation industry, often based around the size of the particular airport. Tensions existed in relation to matters such as the cost and practical implications of instituting the changes. In providing advice to the Minister, OTS sought to strike a balance between the desired security outcomes and the practical implications of any proposed regulatory changes.

5.43 There is evidence that advice provided by industry participants was incorporated into the proposed regulatory changes. OTS also relied on elements of their compliance activities that had identified issues relating to VIC non-compliance as widespread across the industry. Under the current legislative regime there are potential legal impediments to requiring VIC issuing bodies to provide OTS actual data of VIC usage for policy development purposes. OTS did not explore options for obtaining a sample of VICs on a voluntary basis and, consequently was not in a position to undertake any specific analysis of VIC usage in the design of the proposed changes. For this reason, OTS was required to rely heavily on industry representations and anecdotal evidence. A consequence of this approach is that OTS was unable to accurately assess the security outcomes of potential proposed changes. Going forward, it will be important that OTS's information gathering powers are sufficient to enable objective monitoring of the proposed visitor management scheme, following amendments to the ATS Regulations.

5.44 To provide some context to the incidence of VIC use the ANAO conducted some analysis around the issue of VICs. In particular, the ANAO worked closely with one gateway airport obtaining de-identified data on a voluntary basis. While relating to only one airport, the analysis provides an insight into current VIC usage.

5.45 The airport selected was one of Australia's largest airports. The work was conducted with the airport operator and did not include other issuing bodies onsite, of which there are five, that also have the ability to issue VICs. As a consequence, the work conducted by the ANAO provides a segment of the total potential VIC population. The airport has a range of mechanisms to manage VICs, including three separate computerised systems and 23 agents who manage paper-based registers. The ANAO obtained de-identified extracts

from two of the computerised databases. The databases included VICs issued to delivery vehicle drivers from various gates as well as electronic VICs issued to individuals—it did not include VICs issued by agents.

5.46 From the available sources, in 2009–10 the selected airport issued 79 304 VICs to 25 155 individuals, and 80 per cent of the VICs issued were to individuals who had multiple visits.

5.47 The ANAO also conducted some specific analysis of the database that was used for VICs issued for vehicle delivery drivers (and their passengers) at one gate at the selected airport. Table 5.1 shows that 42 169 VICs were issued in 2009–10 to 7443 visitors. Of these visitors, 2958 accessed the airport on more than one occasion. In total, these 2958 visitors were issued over 37 000 VICs—around 90 per cent of the VICs issued. There was one example of an individual being issued 1069 separate VICs in 2009–10.

Table 5.1

Number and incidence of VICs issued to individuals in 2009–10 at a delivery gate of the selected airport

Visits per person using VICs	1	2-10	11-28	29+	Total
Number of visitors using VICs	4485	2217	445	296	7443
Number of VICs issued to these visitors	4485	8563	7574	21547	42169
Proportion of total VICs issued to visitors (per cent)	11	20	18	51	100

Source: ANAO analysis of airport data.

5.48 Table 5.1 highlights the substantial use of VICs as a means of regularly accessing secure areas of an airport by individuals who are using the VIC scheme in a systematic manner to gain regular access without the assurance provided by a background check.

5.49 It is a requirement that an issuing body or agent under the VIC scheme must not knowingly issue a VIC to somebody who has been refused an ASIC.[49] However, the ANAO observed that records for ASICs and VICs were often maintained on separate databases, making it difficult for an issuing body to assure itself that it was complying with this requirement. OTS has not specifically assessed this risk and as a consequence no substantive compliance activity has been undertaken in this regard, further reducing the assurance that VICs are only being issued to appropriate individuals.

5.50 Some of the vulnerabilities associated with VICs were identified in the 2004 JCPAA Report 400–*Review of Aviation Security in Australia*. JCPAA reports 406 and 409[50] as well as OTS's commissioned 2008 ASIC legislative review, further highlighted risks and vulnerabilities with the scheme. If implemented, the current proposed changes should address, in part, some of the risks identified in these reviews. However, as at March 2011, none of the risks identified by previous reviews has been addressed. The ANAO's analysis, for one gateway airport, has identified the substantial use of the VIC scheme as a means of gaining regular access to secure areas of an airport. In developing proposed regulatory changes OTS has relied heavily on industry advice, further analysis would provide a more complete understanding of actual VIC usage at key airports.

5.51 The ANAO notes that obtaining de-identified data may not be possible at all locations, and under the current legislative regime it may be difficult to obtain a complete picture of VIC usage. OTS advised that, following the revision to regulations, there may be increased capacity to collect this data as the issuing of VICs will be centralised at airports. OTS would be able to use such data to understand the prevalence and trends in the use of VICs. The outcomes of the analysis would provide a robust basis for the design, and review, of a VIC scheme that addressed the identified vulnerabilities. Determining baseline data will support OTS in monitoring the outcomes of its reforms and assessing whether there are changes in the behaviour of industry participants that address the indentified vulnerabilities.

---

[49] ATS Regulations 6.38 (6).

[50] JCPAA Report 406–*Developments in Aviation Security since the Committee's June 2004 Report 400: Review of Aviation Security in Australia–An Interim Report* (2005) and JCPAA Report 409–*Developments in Aviation Security Since the Committee's June 2004 Report 400: Review of Aviation Security in Australia* (2006).

Recommendation No.3

5.52 To improve the effectiveness of the ASIC scheme, the ANAO recommends that, following implementation of the revised visitor management regulations, OTS monitors the actual usage of visitor identification cards at security controlled airports and uses this information to inform the ongoing development of the ASIC scheme and compliance activity.

DIT response: *Agreed*

5.53 Appendix 1 sets out DIT's complete response to the recommendation.

Ian McPhee
Auditor-General

Canberra ACT
5 May 2011

Appendices

Appendix 1: Agencies' responses

Attorney-General's Department

The Department welcomes the ANAO's report on the processes and systems AusCheck has in place to ensure it carries out a high quality and accountable background checking system.

The proposed report highlights issues around data discrepancies within the AusCheck database. In particular, the data set out in table 4.1 notes the variations that can exist between holdings in the AusCheck database, and holdings by individual Issuing Bodies. These often arise where activities are legitimately undertaken by an Issuing Body, but the body does not update the AusCheck database to reflect that activity. While the proposed report correctly notes that Issuing Bodies are the responsibility of OTS, AusCheck is keen to work with both OTS and the Issuing Bodies to reduce this issue. AusCheck is currently exploring whether there are changes that can be made to the AusCheck System to assist with the problem of cards being marked by AusCheck as 'issued' before they are actually issued by issuing bodies. Enhancing the ability to cancel cards in the system is also being explored.

AusCheck operates a 'help desk' (via phone and email) to assist Issuing Bodies in their use of the AusCheck System. AusCheck is committed to extending this assistance through running a series of face to face meetings with officers from the Issuing Bodies, and providing further written material about the AusCheck system. These activities should assist Issuing Bodies with understanding how to meet their responsibilities in the AusCheck system, and also provide an opportunity to highlight other aspects of the system.

One aspect of the system AusCheck has been working to highlight is the Card Verification Service (CVS). The proposed report notes both the usefulness, and the lack of widespread understanding, of the CVS. The CVS essentially enables people working in areas where ASICs and MSICs are to be worn to verify online the authenticity of a security card presented by an individual.

The proposed report also highlights the issue around the upload of photographs of MSIC and ASIC holders into the AusCheck system. AusCheck is continuing to work closely with Issuing Bodies on this important issue, and has continued to see improvements in the statistics.

Aus Check will continue to raise issues, and explain features of the AusCheck system with members at its regular consultative committee meetings.

Department of Infrastructure and Transport

DIT welcomes the Performance Audit into the management of the ASIC and MSIC schemes, and notes the positive comments made about a range of matters including DIT's approach to industry consultation, governance and risk management.

Over the past five years, the Government's approach to managing identity security on airports and seaports has been in a process of ongoing continual improvement, which has seen a number of important enhancements, including:

- The establishment of the MSIC scheme, where previously people working in sensitive maritime areas had no government mandated background checking;
- The establishment of AusCheck as a government agency providing a robust, consistent and efficient approach to background checking;
- An increase in audit and compliance activity relating to those industry participants responsible for issuing cards; and
- A significant tightening of the MSIC by broadening the range of offences that might preclude a person from MSIC eligibility.

Further enhancements to the ASIC scheme arising from the National Aviation Policy White Paper including a tightening of visitor management arrangements on airports, and a reduction in issuing body numbers are close to finalisation after extensive industry consultation.

DIT recognises this report as a valuable contribution to the ongoing continuing process of the ASIC and MSIC schemes. As such, DIT agrees with all three recommendations in the report, and has already started implementing the first two recommendations by:

- Commencing an assessment of the generic risks and vulnerabilities associated with issuing body practices as they relate to the card application and issuance processes; and
- In preparing the 2011-12 national compliance program DIT is:
  - Giving increased priority to higher risk issuing bodies;

- Revising processes used to analyse compliance findings to better inform future activity;
- Amending inspection tools to ensure all identity cards issued meet legislative requirements; and
- Amending the OTS Compliance Manual and inspector induction training to improve the consistency and usefulness of observations made by staff during compliance activity.

In respect of the last recommendation, DIT will undertake a post implementation review in line with good regulatory practice. This will occur after the new visitor management arrangements have been introduced and the new IT systems and processed are properly established. At this time, DIT will seek depersonalised data not currently available on a range of issues, including the frequency of the attendance of visitors at airports, to assess the effectiveness of the new regulatory settings.

DIT also notes other observations about the ASIC and MSIC schemes, and intends to:

- Work in partnership with AusCheck (as the lead agency on this issue) to reduce inconsistencies between AusCheck's and issuing bodies' databases; and
- Conduct an environmental scan to look at options (including new or improved technology) to address potential risks associated with the non-return of expired ASICs and MSICs.

DIT would like to thank the ANAO and its staff for this report.

Appendix 2: Aviation and maritime-security-relevant offences

Aviation

ATS Regulation 6.01 (2)

A person has an ***adverse criminal record*** if the person has been convicted of:

(b) an aviation-security-relevant offence and sentenced to imprisonment; or

(c) two or more aviation-security-relevant offences (with no imprisonment) one of which was received within 12 months of the criminal history check.

ATS Regulation 6.01 (3)

A person has a ***qualified criminal record*** if the person:

(a) has been convicted twice or more of aviation-security-relevant offences; and

(b) did not receive a sentence of imprisonment for any of those convictions; and

(c) did not receive any of those convictions within the 12 months ending on the date when the relevant background check was conducted.

ATS Regulation 6.28 (abbreviated)

An issuing body must not issue an ASIC to an individual if a person has an ***adverse criminal record.*** An issuing body may issue an ASIC to a person with a ***qualified criminal record*** on the condition that the person must have a further background check conducted within twelve months.

ATS Regulation 6.01

Aviation-security-relevant offence means an offence of a kind mentioned in the Table A.1 against a law of the Commonwealth, or of a State or Territory, or of any other country or part of a country.

Table A 1

Aviation-security-relevant offences

Item	Kind of Offence
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 II of the Crimes Act 1914, against the Government of: (a) the Commonwealth or a State or Territory; or (b) 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

Source: ATS Regulation 6.01.

Maritime

MTOFS Regulation 6.08A

A person has an ***adverse criminal record*** if he or she has been convicted of a maritime-security-relevant offence and sentenced to imprisonment (including periodic detention, home-based detention, and detention until the rising of the court, but not including a sentence of community service).

MTOFS Regulation 6.07B

Maritime-security-relevant offence means an offence relating to a matter mentioned in an item in Table A2 against a law of:
(a) the Commonwealth, a State or Territory; or
(b) a foreign country or part of a foreign country.

MTOFS Regulations—Schedule 1 Maritime-security-relevant-offences

Note 1 A person convicted of an offence mentioned in Part 1 Table A2 is disqualified from holding an MSIC but, under subregulation 6.08X (6), is entitled to seek reconsideration of the decision to issue a disqualifying notice.

Note 2 An issuing body must not issue an MSIC to a person who has been convicted of an offence mentioned in Part 2 of Table A2 and sentenced to imprisonment unless the Secretary, acting under regulation 6.08F, approves the issue of an MSIC to the person.

Table A 2

Maritime-security-relevant offences

Item	Part 1—Disqualifying offences
1.1	terrorism
1.2	treason, sedition, espionage or selling national secrets
1.3	weapon of mass destruction
1.4	hijacking or destruction of an aircraft, vessel or offshore facility

Item	Part 2—Other maritime-security-relevant offences
2.1	armed attack relating to aircraft, airport, vessel, port or offshore facility
2.2	unlawful interference with maritime transport, offshore facility or aviation
2.3	threat to endanger aircraft, airport, vessel or port
2.4	theft of aircraft or vessel
2.5	piracy
2.6	assassination, murder, attempted murder or manslaughter
2.7	threat to murder
2.8	aggravated assault including the following, whether or not the assault results in injury: grievous bodily harm actual bodily harm torture wounding aggravated sexual assault assault with use of weapon assault in company
2.9	kidnapping
2.10	hostage-taking, deprivation of liberty or false imprisonment
2.11	people smuggling or people trafficking
2.12	racial hatred or racial vilification
2.13	affray or riot
2.14	arson or sabotage
2.15	threat to cause fire or explosion
2.16	unlawful activity relating to weapons, firearms or explosives (not including weapons of mass destruction)
2.17	armed robbery
2.18	destruction of or damage to property belonging to the Commonwealth
2.19	threat to destroy or damage property belonging to the Commonwealth
2.20	hinder or resist government officer concerned with national security
2.21	bribery or corruption
2.22	extortion, blackmail or racketeering
2.23	money laundering
2.24	false testimony, perjury or subverting the course of justice

Item	Part 2—Other maritime-security-relevant offences
2.25	forgery or fraud, including identity fraud
2.26	supply false documentation to get a weapons, explosives or vehicle licence
2.27	unlawful activity relating to passports or visas
2.28	impersonate, misrepresent or falsely advertise a profession or professional status
2.29	deceptive business practice
2.30	import, export, supply, manufacture or cultivate illegal drug or controlled substance
2.31	permit premises to be used for taking, selling or distributing illegal drugs or controlled substances
2.32	conspiracy to commit an offence related to a matter mentioned in items 1.1 to 1.4 and 2.1 to 2.31.

Source: MTOFS Regulations Schedule 1.

Appendix 3: ASIC and MSIC issuing bodies

Table A 3

List of ASIC issuing bodies

List of ASIC Issuing Bodies				
Adelaide Airport	Airservices Australia	Albany Airport	Albury Airport	Airport Security Pty Ltd
Alice Springs Airport	Argyle Airport	Armidale Regional Airport	Aurukun Airport	Australian Customs and Border Protection Service
Avalon Airport Australia	Aviation ID	Ayers Rock Airport	Badu Island Airport	Ballina Byron Gateway Airport
Bamaga / Injinoo Airport (Northern Peninsula Airport)	Barcaldine Airport	Bathurst Regional Airport	Bathurst Island Airport	Bedourie Airport
Birdsville Airport	Blackall Airport	Blackwater Airport	Boigu Island	Boulia Airport
Bourke Airport	Brisbane Airport	Broken Hill Airport	Broome International Airport	Bundaberg Airport
Burketown Airport	Burnie Airport	Cairns International Airport	Cambridge Aerodrome	Canberra Airport
Carnarvon Airport	Civil Aviation Safety Authority	Ceduna Airport	Charleville Airport	Christmas Island Airport
Cloncurry Aerodrome	Cobar Airport	Cobham Flight Operations & Services	Coconut Island Airport	Cocos (Keeling) Islands Airport
Coen Aerodrome	Coffs Harbour Regional Airport	Coober Pedy Airport	Cooktown Aerodrome	Cooma-Snowy Mountains Airport
Coonamble Aerodrome	Cunnamulla Airport	Curtin Domestic Aerodrome	Darnley Island Airport	Darwin International Airport
Derby Airport	Devonport Airport	Doomadgee Airport	Dubbo City Airport	Elcho Island Airport
Emerald Airport	Esperance Airport	Essendon Airport	Fitzroy Crossing Airport	Flinders Island Aerodrome
Forte Airport Management	Garden Point Airport	Geraldton Airport	Gladstone Airport	Gold Coast Airport

List of ASIC Issuing Bodies				
Gove Airport	Grafton Airport	Griffith Airport	Groote Eylandt Airport	Halls Creek Airport
Hamilton Airport	Hamilton Island Airport	Hervey Bay Airport	Hobart International Airport	Horn Island Airport
Hughenden Airport	Iama Airport (Yam Island)	Illawarra Regional Airport (Wollongong Aerodrome)	Inverell Airport	Julia Creek Airport
Kalbarri Airport	Kalgoorlie-Boulder Airport	Kalkgurung Airport	Karratha Airport	Karumba Airport
Katherine/Tindal Airport	King Island Aerodrome	Kingscote Aerodrome	Kowanyama	Kununurra Airport
Lajamanu Hooker Creek Airport	Lake Evella Airport	Latrobe Regional Airport	Launceston Airport	Laverton Aerodrome
Learmonth Airport	Leinster Aerodrome	Leonora Airport	Lismore Regional Airport	Lockhart River Aerodrome
Longreach Aerodrome	Lord Howe Island Aerodrome	Mabuiag Island Airport	Mackay Airport	Maningrida Airport
McArthur River Airport	Meekatharra Airport	Melbourne Airport	Mildura Airport	Milingimbi Airport
Moorabbin Airport	Moranbah Aerodrome	Moree Airport	Mornington Island	Moruya Airport
Mount Hotham Airport	Mount Isa Airport	Mt Gambier and District Airport	Mt Magnet Airport	Mudgee Airport
Murray Mer Island	Narrabri Aerodrome	Narrandera Aerodrome	Newcastle Airport	Newman Airport
Norfolk Island Airport	Normanton Airport	Numbulwar Airport	Olympic Dam Airport	Orange Aerodrome
Palm Island Airport	Paraburdoo Airport	Parkes Regional Airport	Perth Airport	Pormpuraaw Aerodrome
Port Augusta	Port Hedland International Aerodrome	Port Keates Aerodrome	Port Lincoln Airport	Port Macquarie Airport
Portland Airport	Qantas	Quilpie Airport	Recreation Aviation Australia Inc.	Ramingining Airport
Ravensthorpe Airport	Royal Flying Doctor Service of Australia	Richmond Aerodrome	Rockhampton Airport	Roma Airport

List of ASIC Issuing Bodies				
Saibai Island Airport	Shark Bay Airport	Snake Bay Airport	St George Aerodrome	Sunshine Coast Airport
Sydney Airport	Tamworth Regional Airport	Taree Airport	Tennant Creek Airport	Thangool Aerodrome
Thargomindah Aerodrome	Toll Priority	Toowoomba Airport	Townsville Airport	Victoria River Downs Airport
Virgin Blue Airlines	Wagga Wagga Airport	Warraber Island Airport	Wees Nawia Airport (Kubin / Moa Island)	Weipa Aerodrome
West Wyalong Aerodrome	Whitsunday Coast Airport	Whyalla Airport	Wiluna Airport	Windorah Airport
Winton Airport	Yorke Island Airport			

Source: ANAO analysis of information held by OTS.

Note: The ANAO used the commonly referred name for some Issuing Bodies, for example Sydney Airport represents Sydney Airport Corporation Ltd.

Table A 4

List of MSIC issuing bodies

List of MSIC Issuing Bodies		
1-Stop Connections Pty Ltd	Albany Port Authority	Australian Amalgamated Terminals
Australian Customs and Border Protection Service	Bunbury Port Authority	Chubb Electronic Security (WA)
ClientView Pty Ltd	Dampier Port Authority	DP World
Esperance Port Authority	Fastcards Pty Ltd	Fremantle Port Authority
Geraldton Port Authority	Pacific National Pty Ltd	Patrick Corporation
Port Hedland Port Authority	Port of Brisbane	Sydney Ports Corporation
Total Marine Services	Veritas Engineering Pty Ltd	

Source: ANAO analysis of information held by OTS.

Appendix 4: Security regulated airports

Table A 5

Australian security regulated airports

List of Australian security regulated airports				
Adelaide	Albany	Albury	Alice Springs	Archerfield
Argyle	Armidale	Aurukun	Avalon	Ayers Rock
Badu Island	Ballina	Bankstown	Barcaldine	Bathurst
Bathurst Island	Bedourie	Belmont	Birdsville	Blackall
Blackwater	Boigu Island	Boulia	Bourke	Brisbane
Broken Hill	Broome	Bundaberg	Burketown	Burnie
Cairns	Cambridge	Canberra	Carnarvon	Ceduna
Charleville	Christmas Island	Cloncurry	Cobar	Coconut Island / Poruma
Cocos (Keeling) Island	Coen	Coffs Harbour	Coober Pedy	Cooktown
Cooma-Snowy Mountains	Coonabarabran	Coonamble	Cunnamulla	Curtin
Darnley / Erub Island	Darwin	Derby	Devonport	Doomadgee
Dubbo	Elcho Island	Emerald	Esperance	Essendon
Fitzroy Crossing	Flinders Island	Garden Point	Geraldton	Gladstone
Gold Coast	Gove	Grafton	Griffith	Groote Eylandt
Halls Creek	Hamilton	Hamilton Island	Hervey Bay	Hobart
Horn Island	Hughenden	Iama (Yam Island)	Illawarra (Wollongong)	Inverell
Jandakot	Julia Creek	Kalbarri	Kalgoorlie-Boulder	Kalkgurung / Kalkaringi
Kambalda	Karratha	Karumba	Katherine - Tindal	King Island
Kingscote	Kowanyama	Kununurra	Lajamanu Hooker Creek	Lake Evella
Latrobe	Launceston	Laverton	Learmonth	Leinster
Leonora	Lismore	Lockhart River	Longreach	Lord Howe Island
Mabuiag Island	Mackay	Maningrida	McArthur River Mine	Meekatharra
Melbourne	Merimbula	Middlemount	Mildura	Milingimbi

List of Australian security regulated airports				
Moorabbin	Moree	Mornington Island	Moruya	Mount Hotham
Mount Isa	Mt Gambier	Mt Magnet	Mudgee	Murray Island
Narrandera	Newcastle	Newman	Norfolk Island	Normanton
Northern Peninsula	Numbulwar	Olympic Dam	Orange	Palm Island
Paraburdoo	Parafield	Parkes	Perth	Pormpuraaw
Port Augusta	Port Hedland	Port Keats	Port Lincoln	Port Macquarie
Portland	Quilpie	Ramingining	Ravensthorpe	Richmond
Rockhampton	Roma	Saibai Island	Shark Bay	Snake Bay
St George	Sunshine Coast	Sydney	Tamworth	Taree
Tennant Creek	Thangool	Thargomindah	Toowoomba	Townsville
Victoria River Downs	Wagga Wagga	Warraber Island	Warrnambool	Weipa
Wees Nawia (Kubin / Moa Island)	Whitsunday Coast	Whyalla	Wiluna	Windorah
Winton	Yorke Island			

Source: ANAO analysis of government gazettes published on Attorney-General's website from January 2005 to October 2010.

Appendix 5: Security regulated maritime areas

Table A 6

Australian security regulated maritime areas

List of Australian regulated security maritime areas				
List of Australian security regulated ports				
Abbott Point	Adelaide	Albany	Alma	Ardrossan
Barrow Island	Bing Bong	Bonython	Brisbane	Broome
Bunbury	Bundaberg	Burnie	Cairns	Cape Flattery
Carnarvon – Cape Cuvier	Carnarvon – Useless Loop	Christmas Island	Cockatoo Island, Yampi Sound	Cocos (Keeling) Island
Corner Inlet and Port Albert	Dampier	Darwin	Derby	Devonport
Eden	Esperance	Fremantle	Geelong	Geraldton
Giles	Gladstone	Gove	Grassy	Groote Eylandt
Hastings	Hay Point and Dalrymple Bay	Hedland	Hobart	Karumba
Kembla	Koolan Island	Lady Barron	Latta	Launceston
Lincoln	Lucinda	Mackay	Melbourne	Melville Island
Mourilyan	Newcastle	Norfolk Island	Onslow – Airlie Island	Onslow – Beadon Point
Onslow – Thevenard Island	Pirie	Point Wilson	Port Botany	Port Jackson
Portland	Spring Bay	Thevenard	Thursday Island	Townsville
Varanus Island	Walcott	Wallaroo	Weipa	Whyalla
Wyndham	Yamba	Yelcher Beach		
List of Australian security regulated offshore facilities				
Agincourt	Angel	Barracouta	Basker Spirit	Bream A
Bream B	Campbell	Challis Venture	Cliff Head A	Cobia
Cossack Pioneer	Cowle	Crystal Ocean	Dampier Spirit	Dolphin
Double Island	Flounder	Fortescue	Four Vanguard	Front Puffin
Gibson / South Plato	Goodwyn Alpha	Griffin Venture	Halibut	Harriet A
Harriet B	Harriet C	Jabiru Venture	John Brookes	Karratha Spirit

List of Australian security regulated offshore facilities				
Kingfish A	Kingfish B	Linda	Mackerel	Maersk Ngujima-Yin
Marlin	Modec Venture 11	Nganhurra	North Rankin Alpha	Northern Endeavour
Ocean Legend	Perch	Pyrenees Venture	Roller A	Roller B
Roller C	Saladin A	Saladin B	Saladin C	Simpson A
Simpson B	Sinbad	Skate	Snapper	Stag A
Stybarrow Venture MV-16	Thylacine A	Tuna	Twickenham	Victoria
Wandoo A	Wandoo B	Wandoo CALM Buoy	West Kingfish	West Tuna
Whiting	Wonnich	Yammaderry A	Yolla A	

Source: ANAO analysis of government gazettes published on Attorney-General's website from January 2005 to October 2010.

Index

Series Titles

ANAO Audit Report No.1 2010–11
Implementation of the Family Relationship Centres Initiative
Attorney-General's Department
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.2 2010–11
Conduct by Infrastructure Australia of the First National Infrastructure Audit and Development of the Infrastructure Priority List
Infrastructure Australia

ANAO Audit Report No.3 2010–11
The Establishment, Implementation and Administration of the Strategic Projects Component of the Regional and Local Community Infrastructure Program
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.4 2010–11
National Security Hotline
Australian Security Intelligence Organisation
Attorney-General's Department
Australian Federal Police

ANAO Audit Report No.5 2010–11
Practice Incentives Program
Department of Health and Ageing
Medicare Australia

ANAO Audit Report No.6 2010–11
The Tax Office's implementation of the Client Contact - Work Management - Case Management System
Australian Taxation Office

ANAO Audit Report No.7 2010–11
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2009 Compliance)

ANAO Audit Report No.8 2010–11
Multifunctional Aboriginal Children's Services (MACS) and Crèches
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.9 2010–11
Green Loans Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency

ANAO Audit Report No.10 2010–11
Centrelink Fraud Investigations

ANAO Audit Report No.11 2010–11
Direct Source Procurement

ANAO Audit Report No.12 2010–11
Home Insulation Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency
Medicare Australia

ANAO Audit Report No.13 2010–11
Implementation and Administration of the Civil Aviation Safety Authority's Safety Management System Approach for Aircraft Operators

ANAO Audit Report No.14 2010–11
Capitalisation of Software
Australian Bureau of Statistics
Civil Aviation Safety Authority
IP Australia

ANAO Audit Report No.15 2010–11
Food Standards Australia New Zealand

ANAO Audit Report No.16 2010–11
Centrelink's Role in the Process of Appeal to the Social Security Appeals Tribunal and to the Administrative Appeals Tribunal
Centrelink
Department of Education, Employment and Workplace Relations
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.17 2010–11
2009–10 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.18 2010–11
Government Business Managers in Aboriginal Communities under the Northern Territory Emergency Response
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.19 2010–11
Army Aboriginal Community Assistance Program
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.20 2010–11
Administration of the Wine Equalisation Tax
Australian Taxation Office

ANAO Audit Report No.21 2010–11
Indigenous Housing Initiatives: the Fixing Houses for Better Health program
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.22 2010–11
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2010

ANAO Audit Report No.23 2010–11
Home Ownership of Indigenous Land Program
Department of Families, Housing, Community Services and Indigenous Affairs
Indigenous Business Australia

ANAO Audit Report No.24 2010–11
The Design and Administration of the Better Regions Program
Department of Regional Australia, Regional Development and Local Government

ANAO Audit Report No.25 2010–11
Administration of the Trade Training Centres in Schools Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.26 2010–11
Management of the Tender Process for a Replacement BasicsCard
Department of Human Services

A**NAO Audit Report No.27 2010–11**
Restoring the Balance in the Murray-Darling Basin
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.28 2010–11
Management of the Australian Broadband Guarantee Program
Department of Broadband, Communications and the Digital Economy

ANAO Audit Report No.29 2010–11
Management of the Implementation of New Policy Initiatives
Australian Federal Police

ANAO Audit Report No.30 2010–11
Digital Education Revolution Program—National Secondary Schools Computer Fund
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.31 2010–11
Administration of the Superannuation Lost Members Register
Australian Taxation Office

ANAO Audit Report No.32 2010–11
Northern Territory Night Patrols
Attorney-General's Department

ANAO Audit Report No.33 2010–11
The Protection and Security of Electronic Information Held by Australian Government Agencies

ANAO Audit Report No.34 2010–11
General Practice Education and Training
General Practice Education and Training Limited

ANAO Audit Report No.35 2010–11
Management of the Overseas Leased Estate
Department of Foreign Affairs and Trade

ANAO Audit Report No.36 2010–11
Service Delivery in CRS Australia
Department of Human Services

ANAO Audit Report No.37 2010–11
Management of Explosive Ordnance Held by the Air Force, Army and Navy
Department of Defence

ANAO Audit Report No.38 2010–11
Management of the Certificate of Compliance Process in FMA Act Agencies

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office website.

Human Resource Information Management Systems	
Risks and Controls	Mar 2011
Fraud Control in Australian Government Entities	Mar 2011
Strategic and Operational Management of Assets by Public Sector Entities –	
Delivering agreed outcomes through an efficient and optimal asset base	Sep 2010
Implementing Better Practice Grants Administration	June 2010
Planning and Approving Projects	
an Executive Perspective	June 2010
Innovation in the Public Sector	
Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0	
Security and Control	June 2009
Preparation of Financial Statements by Public Sector Entities	June 2009
Business Continuity Management	
Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006

Legal Services Arrangements in Australian Government Agencies	Aug 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006