Australian Government

Department of Infrastructure, Transport,
Regional Development and Local Government

Department of Infrastructure, Transport, Regional Development and Local Government

SUBMISSION TO THE

PARLIAMENTARY JOINT COMMITTEE ON THE AUSTRALIAN CRIME COMMISSION

INQUIRY INTO THE ADEQUACY OF AVIATION AND MARITIME SECURITY MEASURES TO COMBAT SERIOUS AND ORGANISED CRIME

November 2009

Introduction

The Department of Infrastructure, Transport, Regional Development and Local Government (the Department) contributes to the wellbeing of all Australians by fostering an efficient, sustainable, competitive, safe and secure transport system. Through the Department the Office of Transport Security (OTS) contributes to these outcomes by continually working to maintain and enhance a transport system that is more secure against the threat of terrorism and unlawful acts.

The purpose of this submission is to illustrate the Department's role in regard to the administration and operation of the Australian Government's preventive aviation and maritime security regimes, including specific components of these regimes such as the Aviation and Maritime Security Identification Card schemes. This paper also outlines the specific regulatory measures currently in place to mitigate the threat of terrorism to Australia's aviation and maritime sectors.

The security environment

Following the events of 11 September 2001 there was a significant increase in focus on mitigating threats posed by international terrorism, especially in the transport sector.

Terrorist groups have demonstrated the intent and capability to mount successful attacks against transportation systems around the world and, owing to the nature of operations, transport systems provide opportunities to meet terrorist objectives of inflicting mass casualties, causing significant economic damage, instilling fear, and creating spectacular media imagery.

The main threat to Australia and its interests overseas continues to come from those who are part of, or inspired by, the global terrorist movement. Australian aviation and maritime industries are potentially vulnerable to attack by terrorists.

While Australia's intelligence and police organisations are working together to prevent terrorist activity, and may uncover evidence of an impending attack, it is not prudent to assume they will be able to identify and resolve all possible threats. It is possible that an attack against Australia or Australian interests could occur without any prior intelligence warning.

Due to the potentially unpredictable environment, the Australian Government relies on a strong prevention and preparedness regime as the first step in its broader counter-terrorism strategy, as outlined in the National Counter-Terrorism Plan (NCTP). This strategy encompasses targeted prevention measures based on risk management principles as outlined in the risk management standard Australian/New Zealand Standard 4360/2004 (AS/NZS4360) and the accompanying Security Risk Management Handbook 167:2006 (HB 167).

This approach recognises that efficient, safe and secure aviation and maritime transport systems are integral to Australia's economic wellbeing. The Government is committed to ensuring Australia's security regimes are focused, proportional and suitable while addressing threats faced in each transport sector. It is important to review threats to national security continually, to identify key vulnerabilities, and to revise system and policy settings where appropriate considering the impacts on the transport sector and the potential security benefits. Security measures should not be a barrier to ease of travel, nor prevent the facilitation of trade either domestically or internationally.

Government response

Australia's aviation and maritime security regimes have been significantly strengthened in response to terrorist attacks since 11 September 2001. The Australian Government continues to work with State and Territory governments and industry to improve the security of Australia's transport system and reduce the likelihood of transport being a target or used as a vehicle for terrorism.

Working within the NCTP, the Australian Government sets and enforces a preventive security framework for the aviation, air cargo and maritime industries. These frameworks provide strong, flexible and responsive preventive security measures which reduce the likelihood that Australia's aviation and maritime transport systems will be a target of, or used to facilitate, a terrorist act.

The risk management principles utilised as the basis for the Australian Government's approach to preventive security revolves around the requirement for industry operators to first identify security vulnerabilities in their operating environments, and then to implement appropriate measures to mitigate those identified vulnerabilities. Identifying such vulnerabilities is crucial to preventive security. Vulnerabilities potentially amplify terrorist capabilities and increase the likelihood of an attack occurring.

Internationally the Australian Government works as a member of the International Civil Aviation Organization and the International Maritime Organization (IMO) to ensure an internationally coordinated response to transport security measures. The presence of these international bodies, and Australia's participation in them, recognises that terrorism is a transnational challenge. Combating terrorism requires both national and international cooperation and coordination.

In December 2002 the IMO developed the International Ship and Port Facility Security (ISPS) Code in response to the international community's resolve to implement a system to secure the maritime transport sector against the threat of terrorism. The preventive security framework implemented by the Australian Government in the maritime sector reflects the preventive security requirements set out in the ISPS Code.

The preventive security framework implemented by the Australian Government in the aviation sector reflects Australia's obligations under the Convention on International Aviation (also known as the Chicago Convention). Annex 17 of the Chicago Convention sets out the standards that signatory states such as Australia are required to comply with in order to safeguard international aviation from the threat of terrorism. Although in existence since 1974, amendments to annex 17 were made in December 2001 in order to address challenges posed to civil aviation following the terrorist acts of 11 September 2001. The new amendments commenced on 1 July 2002.

Roles of regulator and industry

The Department, through OTS, is the primary advisor to the Australian Government on transport security policy and is the transport security regulator. OTS was established as a business division of the Department in 2004.

Prior to OTS' establishment, there was no single regulator responsible for securing Australia's aviation and maritime sectors from the threat of terrorism. The creation of OTS, and development of the specific national security legislation applying to the aviation and maritime sectors, was a significant step in bringing security responsibilities for the aviation

and maritime sectors together in a single national regulatory approach. Since this time OTS has continued to mature, in a changing and unpredictable security environment, into a respectable, well recognised regulator held in high regard by those industries it regulates. As OTS continues to mature so to do its processes and procedures, as well as its ability to regulate.

OTS works closely with the aviation and maritime industries to protect these sectors from the possibility and consequences of a terrorist attack and other forms of unlawful interference. In its role as a preventive security regulator OTS continually seeks to improve preventive security measures, reduce the likelihood of a terrorist act occurring and develop resilience in the aviation and maritime transport sectors. OTS is responsible for administering:

- the *Aviation Transport Security Act 2004* (ATSA) and the Aviation Transport Security Regulations 2005 (ATSR); and
- the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) and the Maritime Transport and Offshore Facilities Security Regulations 2003 (MTOFSR).

In line with Australia's international obligations, these Acts establish the preventive security frameworks for the aviation and maritime sectors, through which OTS regulates industry operators. Industry plays an integral role in securing Australia's aviation and maritime domains by implementing the security regime mandated by these pieces of legislation. The legislative framework established for the aviation and maritime sectors recognises that security is part of doing business in the transport sector. The frameworks were designed in close consultation with industry, considering the different security risk contexts and industry operational environments.

Safeguarding the aviation and maritime industries from the risk of terrorism is a shared responsibility of Government and industry. OTS as the Government regulator works with industry operators to ensure Government's expectations relating to transport security are fully understood and accorded with; this is underpinned by robust audit and compliance arrangements.

OTS recognises that to achieve and maintain high levels of compliance it needs to be open about its processes and strive to ensure industry operators in the same circumstances are treated equitably within the confines of the established security framework.

The elements of the framework in the ATSA and MTOFSA, while broadly similar, differ in some areas. This is a reflection of differing vulnerabilities and risks faced by the two industry sectors. In the context of the current Australian security environment the nature of major aviation operations presents greater inherent vulnerabilities to terrorist threats than the maritime industry. The most attractive opportunities to best meet terrorist objectives in the maritime sector are in relation to passenger vessels and oil and gas operations, which although significant economically, form only a relatively small component of total maritime industry operations in Australia.

Aviation Transport Security Act 2004

The legislated purpose of the ATSA is to "establish a regulatory framework to safeguard against unlawful interference with aviation transport" and to meet "Australia's obligations under the Convention on International Aviation" (ATSA, Section 3). The ATSR provides the detail for this regulatory framework. It sets out the minimum standards that the Government has mandated must be complied with to provide an aviation transport system that is more secure against the threat of terrorism.

Transport security programs

The key mechanism used to achieve this outcome is the requirement for aviation industry participants to develop and comply with transport security programs. A transport security program (TSP) is a preventive security plan that sets out security measures and procedures that must be implemented to reduce the threat of a terrorist act occurring in the aviation sector.

To formulate a TSP, an industry operator must first conduct a security risk assessment of their operation to identify potential security vulnerabilities. They are then required to develop a plan outlining how they will mitigate these vulnerabilities within the legislated security framework. Once implemented, a TSP reduces the risk that an industry participant's operation could be a target of, or used to facilitate, an act of terrorism.

TSPs must contain:

- an outline of the local security risk context, including consideration of location, seasonal and other factors;
- a list of general threats and security risk events and an outline of what must be protected;
- how the operator's aviation security activities will be managed;
- the technology, equipment and procedures to be used to maintain aviation security; and
- how the operator will respond to aviation security incidents.

Airport operators must also include in their security programs mechanisms for consulting between the operator and relevant parties (such as law enforcement agencies) regarding security measures and procedures. In practice this occurs through regular security committee meetings where security related activities and procedures can be communicated. These meetings aim to draw together all key stakeholders within the aviation environment who play a role in the broader security framework to ensure a holistic approach to preventive security and that appropriate coordination arrangements are in place should a security incident occur.

All operators of security controlled airports, operators of prescribed air services and regulated air cargo agents are required to have TSPs. Airservices Australia is also required to have a TSP.

A range of other preventive security mechanisms are created in the ATSA and ATSR to reduce the threat of terrorism, including establishment of security zones, screening and clearing requirements, empowerment of officials to enforce regulatory provisions, the Aviation Security Identification Card scheme, Visitor Identification Cards, and reporting obligations in relation to aviation security incidents. Each of these mechanisms will now be considered in more detail.

Airport areas and zones

Airports designated by the Secretary of the Department as 'security controlled airports' under the legislation (ATSA, Section 28) are subject to security measures which divide the airport into different sections in order to protect critical sections of the airport from the risk of a terrorist act occurring. Such airports include all major metropolitan airports, larger metropolitan General Aviation airports and many regional airports.

A security controlled airport will have an airside and a landside area. The purpose of an airside area is to control access to operational areas of an airport. Any other area within the boundaries of the security controlled airport becomes the landside area. Within airside and landside areas the Secretary may designate specific parts to be airside or landside security zones. The purpose of these zones is to subject the areas covered to stricter or more specialised controls than those applying generally to the airside or landside areas. Such controls may relate to controlling the movement of people in airside areas, restricting access to airside security zones, providing cleared zones or preventing interference with aircraft.

The ATSR authorises the Secretary of the Department to designate sterile areas, usually in an airport terminal building, as a landside security zone. Anyone entering the sterile areas must be screened or exempt from screening requirements. Passengers are required to board their flights directly from the sterile area, to ensure no weapons or prohibited items are carried onto the flight.

Screening and clearing

Access to sterile areas and aircraft is restricted to people, goods and vehicles that have been screened and cleared. Screening is conducted to remove the likelihood of weapons and prohibited items being taken onboard the aircraft or into secure airside zones. All passengers and crew must be screened and cleared before entering a sterile area.

There are some exemptions to the requirement for screening, including law enforcement officers, fire service officers and members of the Australian Defence Force responding to an emergency. Some categories of dignitaries are also exempt from screening, including Heads of State of a country recognised by Australia.

All carry-on baggage and checked baggage must also be cleared before being taken into a sterile area or onto an aircraft to ensure the contents of those bags cannot be used to commit an act of unlawful interference. Vehicles that are to be taken on board an aircraft or into a sterile area in a security controlled airport must also be cleared before being loaded onto the aircraft or before entering the sterile area.

Regulated air cargo agents

Regulated air cargo agents (RACAs) are businesses that handle or make arrangements for the transport of air cargo and are approved by the Secretary, under the ATSA, to operate in this capacity. Regulations affecting RACAs and the air cargo sector commenced from 10 March 2007 were introduced to improve supply chain security for air cargo. RACAs include couriers, freight forwarders, cargo terminal operators at airports, regular international postal services and truck drivers who transport air cargo between cargo terminals. RACAs are responsible for developing and implementing TSPs based on risk assessments of their operations.

There has been a Regulated Agent scheme in place since 1 February 1996, regulating freight forwarders and couriers who security clear international air freight. This scheme was established through regulations under the *Air Navigation Act 1920* to provide a procedure for the security clearance of international air freight and to meet Australia's international obligations.

A restructure of the aviation security system was announced in December 2002. With the commencement of the ATSA and ATSR in early 2005, relevant provisions of the *Air*

Navigation Act 1920 and the *Air Navigation Regulations 1947* were repealed, including the previous Regulated Agent scheme. The ATSA and ATSR now provide a revised regulatory framework for international and domestic air cargo security, with domestic air cargo security being regulated for the first time.

Powers and responsibilities

There are a number of key groups of people who have powers and responsibilities in relation to aviation security and in reducing the risk of a terrorist act occurring at a security controlled airport or on board an aircraft. These people include screening officers, airport security guards, law enforcement officers, and aviation security inspectors.

Screening officers must meet training and qualification requirements and be authorised to conduct screening. Powers granted to screening officers include requesting a person removes items of clothing, frisk searching individuals (with their consent), and the ability to detain and restrain individuals under certain circumstances. Airport security guards must also meet certain training and qualification requirements. Airport security guards are authorised to physically detain and restrain a person if the guard reasonably suspects that the person is committing, or has committed, an offence against the ATSA and the guard believes it is necessary to do so to maintain the integrity of the screening process.

Law enforcement officers include members of the Australian Federal Police or a state or territory police organisation who are on duty at a security controlled airport. A law enforcement officer may enter and remain in any part of a security controlled airport at any time. In addition to their normal powers and responsibilities they are authorised to stop and search people in an airside area, stop and search vehicles in an airside area, request a person to leave an aircraft, area, zone or airport, and remove vehicles from areas and zones.

Officers of the Department as well as law enforcement officers can be appointed as aviation security inspectors by the Secretary of the Department; they have a wide range of powers that they can exercise to determine whether a person is complying with the ATSA. These powers include entering and inspecting any part of a security controlled airport, observing operating procedures, and inspecting, photographing or copying a document or record made by an aviation industry participant. An aviation security inspector can take these actions at a security controlled airport at any time without notice. Inspectors also have powers in relation to aircraft including entering and inspecting the operator's aircraft (however only after giving reasonable notice to the aircraft operator).

Special Security Directions

The ATSA empowers the Secretary of the Department the ability to issue special security directions in response to special circumstances, such as in response to a terrorist threat, that require specific security measures beyond those legislated or set out in an aviation participant's TSP. The Secretary may give such a direction if a specific threat regarding aviation security is made or where there is a change in the nature of an existing general threat to aviation security. Directions can be given to a wide range of people including APS employees of the Department, Airservices officials, aviation industry participants, and aviation passengers.

Control directions

The ATSA also has provision for the issue of control directions; the purpose of these directions is to control the movement of aircraft, where required, and may be given to pilots in command or aircraft operators. There are two types of control directions: compliance control directions, which may be given by an aviation security inspector, and incident control directions which may be issued by the Secretary or transferred to a Secretary or Senior Executive Service Band 3 official of another Government agency with national counter-terrorism responsibilities.

Compliance control directions are designed to ensure compliance with the ATSA and may only be given when an aircraft is not in flight. Actions the operator may be required to take include holding the aircraft in a particular position until a specific event occurs, taking particular actions in relation to a thing on board the aircraft, or allowing an aviation security inspector to inspect the aircraft. In each instance the purpose is to maintain the integrity of the aviation transport system.

Incident control directions may only be given in response to aviation security incidents if the response is necessary or appropriate. They can be given in flight and may include taking particular actions in relation to a person on board the flight, holding the aircraft in a particular position until a specific event occurs, ensuring the aircraft leaves a particular place, or ensuring the aircraft lands at a particular place or outside an area.

Aviation security incidents

Industry participants play an important role in relation to the reporting of aviation security incidents. An aviation security incident may either be actual unlawful interference with aviation, or the threat of unlawful interference with aviation. In broad terms unlawful interference (defined in section 10 of the ATSA) encompasses any act of taking control, damaging or putting safety at risk involving an aircraft or airport.

Anyone who works in the aviation industry has a general responsibility to report aviation security incidents. If an aviation security incident occurs in an airport or in relation to an aircraft, the relevant operator must report it to the Department and relevant police. Aircraft operators must also report incidents to Airservices Australia and the relevant airport operator.

Aviation Security Identification Cards

Overview

In combination with the above preventive security measures, the Aviation Security Identification Card (ASIC) scheme is another layer of security which aims to reduce the risk of potential terrorists infiltrating sensitive areas of aviation infrastructure by excluding people with prior criminal backgrounds relevant to terrorism and serious criminal offences from working in security sensitive areas of the aviation industry.

There are two types of ASICs. A person must display a red ASIC to access the security restricted areas of an airport and either a red or grey ASIC to access to rest of the secure areas. ASICs may apply Australia-wide or may be specific to a particular airport.

The ASIC scheme requires that people working in the security sensitive areas of Australia's aviation sector be background checked. An ASIC is issued to a person who has passed a background check. Anyone working unescorted or unmonitored within secure areas of an airport must have and display an ASIC. These sorts of people include pilots, baggage handlers and aircraft maintenance crew.

The scheme is comparable when benchmarked against countries such as the United Kingdom, Canada and the United States of America.

Development of the ASIC scheme

Prior to 1998 access to federal airports was controlled by the Federal Airports Corporation (FAC). FAC staff were subject to criminal records background checks and were issued with a FAC access card. In December 1998 the ASIC scheme was introduced under the Air Navigation Regulations 1947 (ANR). ASICs were required for the security restricted areas of the major Australian airports. An ASIC required a criminal records check and eligible applicants were issued with a photographic identification card.

Following 11 September 2001, the Australian Government introduced a number of additional measures applying to airports and airlines, including greater controls over access to secure airport areas. The ASIC scheme was subsequently extended to all security controlled airports. Strengthened criteria came into effect in November 2003. Tighter criminal history checks were put in place for new ASIC holders and all ASIC holders were subjected to an ASIO security assessment. Other changes included:

- reducing the validity period of an ASIC from 5 years to 2 years;
- simplifying the application of the spent conviction scheme with the exclusion of certain convictions that were not to be taken as spent for the purposes of ASIC criminal history checks;
- inclusion of items 6, 7 and 8 into the list of aviation-security-relevant-offences;
- permitting issuing bodies to issue Australia wide ASICs (ie for more than one airport)
- introduction of the term 'adverse criminal record';
- requiring ASICs to include a recent photograph, holder's full name, unique number and expiry date; and
- a national re-issue took place in November 2003 to August 2004 to ensure that all ASICs would have newly agreed tamper evident features.

In March 2005 the ASIC scheme was transferred from the ANR to the ATSR. At this time its application was extended to all security controlled airports that received regular public transport services. Eligibility criteria for the ASIC were strengthened in 2006 to include a pattern of criminality test.

Access

ASICs are not access cards and do not automatically confer access rights on the holder to enter the secure areas of airports. These cards merely indicate that the holder has undergone a security related background check and is permitted to be in a secure area in the course of their duties; physical entry to these areas is subject to authorisation of their employer. While some industry participants have attached their own access control arrangements to the ASIC (so their employees are carrying one card instead of two), this

has been done as a matter of convenience. Access controls for airports, at all times, remains the responsibility of airport operators.

Background checking process

To be eligible for an ASIC an individual must have an operational need to access a secure area of a security controlled airport, undergo proof of identity and background checks and satisfy criteria prescribed in the ATSR. A person must undergo a background check every two years for an ASIC. Cards issued are valid for this time unless a lesser period of validity is imposed as a condition of issue.

AusCheck, a Branch of the Attorney-General's Department (AGD), is responsible for coordinating the background checks of ASIC applicants. AusCheck commenced operations on 1 July 2007 following the Right Honourable Sir John Wheeler's 2005 recommendation that a single agency, which he recognised as the AGD, should perform background checking. Prior to AusCheck's commencement this function had been undertaken by the Department.

The background checking process includes:

- a criminal history check facilitated through CrimTrac;
- a security assessment conducted by the ASIO; and, if relevant
- an unlawful non-citizen check conducted by the Department of Immigration and Citizenship.

The process does not involve overseas background checking of applicants.

Eligiblity

A person will be eligible for an ASIC if they satisfy the relevant requirements in the ATSR. The majority of applicants are found ineligible to hold an ASIC result from a failure to pass the criminal history check. The criminal history check involves screening applicants against a predetermined list of 'aviation-security-relevant-offences' as provided at regulation 6.01 of the ATSR. The list of aviation-security-relevant-offences is reproduced below:

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

As per regulation 6.01 of the ATSR, applicants will be found ineligible to hold an ASIC if they have been convicted of:

- an aviation-security-relevant offence and sentenced to imprisonment; or
- two or more aviation-security-relevant-offences (with no imprisonment) one of which was received within 12 months of the criminal history check.

Applicants who do not pass the criminal history check are deemed to have an adverse criminal record. A person with an adverse criminal record is not eligible to be issued with an ASIC.

Also as per regulation 6.01 of the ATSR, a person will have a qualified criminal record if the person:

- has been convicted twice or more of aviation-security-relevant-offences; and
- did not receive a sentence of imprisonment for any of those convictions; and
- did not receive any of those convictions within the 12 months ending on the date.

A person with a qualified criminal record may be issued an ASIC on the condition that the person has a further background check conducted within 12 months after the first background check was conducted.

Appeals

In instances where a person is not eligible to be issued an ASIC because he or she has an adverse criminal record, the applicant's issuing body may apply to the Secretary for reconsideration of the decision not to issue an ASIC.

This is a discretionary process which allows the Secretary to take into account factors that are relevant to a person's eligibility for an ASIC that were not considered during the initial assessment process. These factors, stipulated at regulation 6.29 of the ATSR, are:

- the nature of the offence the person was convicted of;
- the length of the term of imprisonment imposed on him or her;
- if he or she has served the term, or part of the term – how long it is, and his or her conduct and employment history, since the sentence was imposed;
- if the whole of the sentence was suspended – how long the sentence is, and his or her conduct and employment history, since the sentence was imposed; and
- anything else relevant that the Secretary knows about.

It is at the discretion of the issuing body whether or not to lodge a request for review on an applicant's behalf. The Secretary can request the issuing body to provide more information

in order to process the appeal. The Secretary may approve the application subject to conditions, such as more frequent background checking.

In practice, the General Manager, Maritime Identity and Surface Security Branch in the Office of Transport Security will make decisions under regulation 6.29, having been delegated the authority to do so by the Secretary.

Applicants can apply to the Administrative Appeals Tribunal for a review of a decision by the Secretary to refuse the issue of an ASIC pursuant to regulation 6.29.

Exemptions

All individuals who enter security controlled zones within the aviation environment must display a valid ASIC unless an exemption has been authorised by the Department. Regulation 3.08 of the ATSR permits an individual to apply to the Secretary for an exemption to display an ASIC. In addition, the ATSR provides that certain groups of people are automatically exempt from display and use of ASICs including emergency personnel and members of the defence force. Exemptions to display ASICs are commonly issued on the basis of occupational health and safety grounds, especially in relation to aircraft maintenance crew.

Exemption requests are considered to ensure the approval of the request would not undermine the security of Australia's aviation transport system thereby increasing the risk of a terrorist act occurring.

Monitoring of cards issued

ASIC issuing bodies are required to develop and maintain ASIC programs which set out operating procedures in relation to the issue of ASICs. These plans are required to be approved by the Department before the issuing body can commence operations. The program must include procedures with regard to:

- the issue and production of ASICs;
- the safekeeping, secure transport and disposal of ASICs;
- the recovery and secure destruction of issued ASICs that are no longer required;
- lost ASICs; and
- ensuring ASICs are returned to issuing bodies when they are no longer required.

An issuing body is required to keep a register of ASICs issued; the register must contain details of each ASIC issued by the body. These records are auditable by aviation security inspectors. In addition, issuing bodies must provide annual reports to the Secretary at the end of each financial year outlining:

- the total number of ASICs issued by the body that have not expired and have not been cancelled; and
- the number of ASICs issued by the body that have expired or been cancelled but have not been returned to the body.

Issuing bodies are subject to obligations with regard to cancellation of ASICs. An issuing body must cancel an ASIC if:

- the body finds out that the ASIC was not issued in accordance with the body's ASIC program;
- the Secretary of the Department has notified the issuing body in writing that a security assessment of the holder was adverse; or
- the issuing body finds out that the holder has been convicted an offence against Part 2 of the *Crimes (Aviation) Act 1991* or any other aviation-security-relevant-offence for which he or she was sentenced to a term of imprisonment.

Additionally, an issuing body must cancel an ASIC issued by the body if the holder of the ASIC asks the holder to cancel it. The issuing body must notify the Secretary of the Department of this cancellation.

There are also obligations on ASIC holders. The holder of an ASIC must return their card to an issuing body within 1 month of the ASIC expiring, the card being cancelled, or the card being damaged altered or defaced or no longer having an operational need.

The obligations created for issuing bodies and ASIC holders ensure that cards are issued and held in a robust fashion and therefore do not compromise the broader purpose of the ASIC scheme which is to reduce the threat of a terrorist act occurring in the aviation transport system,

Temporary ASICs

The ATSR has provision to allow the issuing of temporary ASICs by issuing bodies. A temporary ASIC can only be issued to a person if his or her card has been lost, destroyed, forgotten or has been stolen. Temporary cards may also be issued where an ASIC has been approved but the issuing body cannot produce the card for a technical reason.

Visitor Identification Cards

The ATSR requires security controlled airport operators to have formal visitor management arrangements in place. This system allows visitors, who may only require 'one off' access to an airport, such as contractors, tour groups, ASIC applicants and other visitors approved by the airport operator or the relevant aviation industry participant responsible for managing access to security areas of airport, to be managed in such a way as to mitigate the potential risks they may pose to aviation security.

The requirement for VIC holders to be supervised at all times by an ASIC holder mitigates potential risks associated with allowing unchecked visitors access to airports. VICs will normally not be issued for longer than one month unless permitted by the issuing body's ASIC program, in which case they can be issued for up to three months. A person who requires a VIC for longer than this time should apply for an ASIC.

Maritime Transport and Offshore Facilities Security Act 2003

The legislated purpose of the MTOFSA is to "safeguard against unlawful interference with maritime transport or offshore facilities" (MTOFSA, Section 3). In doing so the MTOFSA creates minimum security standards which those operating in the maritime industry (defined as 'maritime industry participants) must comply with; these standards aim to ensure that security vulnerabilities are addressed thereby reducing the risk that Australia's maritime transport system will be a target of, or used to facilitate, a terrorist act.

The MTOFSR provides the detail for the security framework established by the MTOFSA. It sets out the minimum standards which the Government has mandated must be complied with to provide a maritime transport system that is more secure against the threat of terrorism. The preventive security framework established by the MTOFSA applies to Australian trading and passenger ships, and foreign ships travelling to a port in Australia. It also applies to Australian ports, port facilities, port service providers and offshore facilities.

Maritime security levels

Unlike the ATSA, the MTOFSA provides for three security levels. These levels, drawn from the ISPS Code, provide an internationally harmonised approach to maritime security levels. The security level is determined in Australia by the Department taking into account the prevailing threat environment. The three maritime security levels are:

- **Security level 1**: This is the default level at which ships, port and offshore facilities normally operate. Security level 1 means the level for which minimum appropriate preventive security measures should be maintained at all times.

- **Security level 2**: This level must be applied when a heightened risk of a security incident is identified. Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

- **Security level 3**: This level is to be applied in exceptional circumstances where there is probable or imminent risk of a security incident. Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident.

Maritime security levels are not the same as those provided for in the National Counter-Terrorism Alert System (consisting of four levels: low, medium, high and extreme). A change in the alert level would not automatically result in a change in security levels and vice versa.

The current maritime security level in Australia is maritime security level 1 for all ports, offshore facilities and Australian regulated ships.

Maritime security plans

Similar to the ATSA, the MTOFSA requires maritime industry participants to develop and comply with security plans to mitigate the threat of terrorism. A maritime security plan (MSP) is a preventive security plan that sets out security measures and procedures that must be implemented to reduce the threat of a terrorist act occurring in the maritime sector.

To formulate a security plan, an industry operator must first conduct a security risk assessment of their operation to identify potential security vulnerabilities. They are then required to develop a plan outlining how they will mitigate these vulnerabilities within the

legislated security framework. Once implemented the plan reduces the risk that the industry participant's operation could be a target of, used to facilitate, an act of terrorism.

It is a legislated requirement that MSPs must:

- reduce the vulnerability of Australian ships, ports, other ships within Australia, and offshore facilities to terrorist attack, without undue disruption to trade; and
- reduce the risk of maritime transport or offshore facilities being used to facilitate terrorist or other unlawful activities.

All security plans must identify the preventive security measures to be taken at each maritime security level Once a higher maritime security level is declared, maritime industry participants—including security regulated foreign ships—must comply with the relevant requirements in their security plans.

Port operators must also include mechanisms in their security plans for consulting with relevant parties (such as port facility operators and law enforcement agencies) regarding security measures and procedures. This occurs through regular security committee meetings where security-related activities and procedures can be communicated. These meetings aim to draw together all key stakeholders within the port or aviation environment who play a role in the broader security framework to ensure a holistic approach to preventive security and ensure appropriate coordination arrangements are in place should a security incident occur.

In addition to the requirement for regulated Australian ships to have security plans, they are also required to have an International Ship Security Certificate (ISSC). The issuing of an ISSC indicates the ship is compliant with the ISPS code; it illustrates to other ISPS member countries that the ship is security compliant thereby ensuring Australia's trading partners have confidence in Australia's maritime transport system.

A range of other mechanisms are created in the MTOFSA to reduce the threat of Australia's maritime transport system being used to facilitate a terrorist act, including the establishment of maritime security zones, screening and clearing requirements, empowerment of officials to enforce regulatory provisions, the Maritime Security Identification Card scheme, and reporting obligations in relation to maritime security incidents. Each of these mechanisms will now be considered in more detail.

Maritime security zones

Maritime security zones are designated by the Secretary of the Department to protect critical areas within security regulated ports, and on or around ships (in port or at sea) or offshore facilities, from the risk of a terrorist act occurring.

Within a security regulated port, the Secretary of the Department can establish one or more port security zones. These can include land-side restricted zones, cleared zones and water-side restricted zones. All port security zones must have security barriers. Barriers for land-side restricted and cleared zones also need to have measures to detect and deny unauthorised access.

Anyone entering a cleared zone must be screened or exempt from screening requirements. Passengers boarding cruise vessels are required to board their vessels directly from the sterile area, to ensure no weapons or prohibited items are carried on board.

Ship security zones can be established around ships within a port or near an offshore facility. The purpose of these zones is to protect the ships within them from the threat of terrorism. Where a port or port facility is expecting a ship considered to be a higher security risk, the port operator may request the Secretary of the Department to declare a ships security zone around that ship.

On-board security zones can be established on regulated Australian ships to create additional security measures, while zones can also be established in or around security regulated offshore facilities. Regardless of where the zone is prepared, its overarching purpose is to reduce the risk that the maritime transport system is used to facilitate a terrorist act.

Maritime industry participants are required to outline the establishment and procedures for maintaining the integrity of security zones in their maritime security plans.

Screening and clearing

Access to cleared zones is restricted to people, goods and vehicles that have been screened and cleared. The key purpose of screening is to prevent anyone taking weapons and prohibited items on board passenger ships. All people, goods, vehicles and vessels (unless exempt) that pass through a screening point to enter a cleared zone have to undergo screening and clearing.

There are some exemptions to the requirement for screening, including law enforcement officers, ambulance or fire service officers, and members of the Australian Defence Force responding to an emergency.

Baggage must also be screened and cleared before being taken into a sterile area or onto a ship to ensure the contents of those bags are not a threat to maritime security. Vehicles and vessels that are to be taken on board a ship or into a cleared zone must also be screened and cleared before being loaded onto the ship or before entering the zone.

Powers and responsibilities

There are a number of key groups of people who have powers and responsibilities in relation to maritime security. These include screening officers, maritime security guards, law enforcement officers, duly authorised officers and maritime security inspectors.

Screening officers must meet training and qualification requirements and be authorised to conduct screening. Powers granted to screening officers include requesting a person remove items of clothing and the ability to detain and restrain individuals under certain circumstances. Maritime security guards must also meet certain training and qualification requirements. Maritime security guards are authorised to physically detain and restrain a person if the guard reasonably suspects that the person is committing, or has committed, an offence against the MTOFSA and the guard believes it is necessary to do so to maintain the integrity of the screening process. Maritime security guards may also remove people, vehicles and vessels from maritime security zones.

Law enforcement officers include members of the Australian Federal Police or a state or territory police organisation who is on duty at a security regulated port or offshore facility. A law enforcement officer may enter and remain in any part of a security regulated port at any time. In addition to their normal powers and responsibilities they are authorised to stop and search people, vehicles and vessels in maritime security zones and to stop and search

people on security regulated ships. In addition, they may remove people, vehicles and vessels from maritime security zones.

The Secretary of the Department may appoint duly authorised officers to inspect the operational areas of a security regulated ship or security regulated offshore facility for the purposes of determining whether a person or a ship is complying with the MTOFSA. People appointed as duly authorised officers could be those who, as part of their regular duties, interact with ship and maritime industry participants, such as customs officers, members of the Australian Defence Force, immigration officers, quarantine officers and Australian Maritime Safety Authority surveyors.

Officers of the Department as well as law enforcement officers can be appointed as maritime security inspectors by the Secretary of the Department; they have a wide range of powers that they can exercise to determine whether a person is complying with the MTOFSA. These powers include inspecting regulated Australian ships' documents for ISSC verification and inspecting ships, offshore facilities, and the premises and operations of industry participants.

Maritime security inspectors can use these powers at any time within the boundaries of a security regulated port or offshore facility.

Security directions

If there is a reason to believe that an unlawful interference with maritime transport or offshore facilities is probable or imminent, the Secretary may issue a security direction requiring additional security measures be implemented over and above those approved in security plans. Security directions can be given to a maritime industry participant, passengers, people within the boundaries of a security regulated port and people within the boundaries of a security regulated offshore facility. Anyone receiving a security direction must comply with its requirements, in addition to those measures currently in place at the existing security level.

In addition to security directions, foreign flagged ships regulated under the MTOFSA may also be issued control directions. Control directions may include removing the ship from Australian waters, removing the ship from a security regulated port, holding position for a specified period of time, or taking particular actions on board the ship.

Maritime security incidents

Industry participants play an important role in relation to the reporting of maritime security incidents. A maritime security incident may either be actual unlawful interference with maritime transport, or the threat of unlawful interference with maritime transport. In broad terms, the term 'unlawful interference' (defined in section 11 of the MTOFSA) encompasses any act of taking control, damaging or putting safety at risk involving a port, ship or offshore facility. Anyone who works in the maritime industry has a general responsibility to report maritime security incidents.

Maritime Security Identification Cards

Overview

In combination with the above mentioned preventive security measures, the Maritime Security Identification Card (MSIC) scheme is another layer of security which aims to reduce the risk of potential terrorists infiltrating sensitive areas of maritime infrastructure by legitimate means by excluding people with prior criminal convictions in terrorism and serious criminal offence categories from working in the security sensitive areas of the maritime and offshore oil and gas industries.

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

The scheme requires that people working in the security sensitive areas of Australia's maritime transport and offshore facilities be background checked. An MSIC is issued to a person who has passed this background check.

Anyone working unescorted or unmonitored within secure areas of a port, ship or offshore oil and gas facility must have and display an MSIC. This includes port workers, stevedores, transport operators such as train and truck drivers, seafarers on Australian regulated ships and people who work on offshore oil and gas facilities.

The MSIC background checking scheme was introduced in 2005. The regulatory provisions underpinning the MSIC regime came into force in the MTOFSR in September 2005 and the requirement to display an MSIC, while working unescorted in a maritime security zone, became fully operational on 1 January 2007.

Access

MSICs are not access cards and do not automatically confer access rights on the holder to enter the secure areas of ports, port facilities, ships or offshore facilities. These cards merely indicate that the holder has undergone a security related background check and is permitted to be in a secure area in the course of their duties; physical entry to these areas is subject to authorisation of their employer. While some industry participants have attached their own access control arrangements to the MSIC (so their employees are carrying one card instead of two), this has been done as a matter of convenience. Access controls for maritime transport and offshore facilities, at all times, remains the responsibility of the operators.

Background checking process

To be eligible for an MSIC an individual must have an operational need to access a secure area of Australia's maritime transport or offshore facilities, undergo proof of identity and background checks and satisfy criteria prescribed in the MTOFSR. A person must undergo a background check every five years for an MSIC. Cards issued are valid for this time unless a lesser period of validity is imposed as a condition of issue.

AusCheck is also responsible for coordinating the background checks of MSIC applicants. As with the ASIC scheme, the background checking process includes:

- a criminal history check facilitated by CrimTrac;

- a security assessment conducted by the ASIO; and, if relevant
- an unlawful non-citizen check conducted by the Department of Immigration and Citizenship.

As with ASICs the process does not involve overseas background checking of applicants.

Eligibility

A person will be eligible for an MSIC if they satisfy all the requirements in the MTOFSR. The majority of applicants found ineligible to hold an MSIC result from a failure to pass the criminal history check. The criminal history check involves screening applicants against a predetermined list of 'maritime-security-relevant-offences' as provided at table 6.07C of the MTOFSR. The list of maritime-security-relevant-offences is reproduced below:

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

Applicants convicted of an offence falling under items 1, 2 or 3 in this table are automatically disqualified from holding an MSIC. Applicants who have been convicted and sentenced to a term of imprisonment for an offence falling under items 4 to 9 are deemed to have an adverse criminal record and are ineligible to hold an MSIC. A person who has been disqualified or found to have an adverse criminal record is not eligible to be issued with an MSIC.

Appeals

Unlike the ASIC appeals process the MSIC regime has a two tier appeal process for applicants who have an adverse criminal record. The first tier is provided by MTOFSR regulation 6.08F, which enables an MSIC issuing body or the applicant to apply to the Secretary, for approval to issue an MSIC.

This is a discretionary process that allows the Secretary to take into account factors that are relevant to a person's eligibility for an MSIC that were not considered during the initial assessment process Before approving or refusing to approve an application, the Secretary must decide whether the person constitutes a threat to the security of maritime transport or an offshore facility by considering the following factors listed at MTOFSR regulation 6.08F:

- the nature of the offence the person was convicted of;
- the length of the term of imprisonment imposed on him or her;
- if he or she has served the term, or part of the term – how long it is, and his or her conduct and employment history, since he or she did so;
- if the whole of the sentence was suspended – how long the sentence is, and his or her conduct and employment history, since the sentence was imposed; and
- anything else relevant that the Secretary knows about.

The Secretary may approve the application subject to conditions, such as more frequent background checking.

In practice, the General Manager, Maritime Identity and Surface Security Branch in the Office of Transport Security will make decisions under regulation 6.08F, having been delegated the authority to do so by the Secretary.

The second appeal tier is enabled by regulation 6.08X of the MTOFSR, which permits an MSIC issuing body or the applicant to apply to the Secretary for further reconsideration, if the appeal under regulation 6.08F was unsuccessful.

This second phase review is assessed by the Office of Transport Security Executive Director and considers all information provided as part of the regulation 6.08F review, and any other additional information which has been provided.

During all phases of the regulatory appeal process, an applicant has the option to appeal the decision to refuse an MSIC, or award an MSIC subject to a condition, directly with the Administrative Appeals Tribunal.

In instances where a person is refused an MSIC because he or she has been disqualified, the applicant or the applicant's issuing body may only apply to the Secretary for reconsideration pursuant to regulation 6.08X.

ASIC holders who apply for an MSIC

MTOFSR regulation 6.08E allows an issuing body to issue an MSIC to an individual who already holds an ASIC, without verifying that they have met the MSIC eligibility criteria requirements.

This is not the case for individuals who hold an MSIC and wish to apply for an ASIC. For such individuals it is still required that they be the subject of a background check to establish

their eligibility under the ASIC scheme. This is because the ASIC eligibility criteria establish a higher threshold for the issue of an ASIC than for an MSIC.

Exemptions

All individuals who enter security controlled zones within the maritime environment must display a valid MSIC unless an exemption has been authorised by the Department. Regulation 6.07M of the MTOFSR permits an individual to apply to the Secretary for an exemption from the requirements to hold, carry or display an MSIC. In addition, the MTOFSR provides that certain groups of people are automatically exempt from display and use of MSICs including emergency personnel and members of the defence force. Exemptions to display MSICs are commonly issued on the basis of occupational health and safety grounds, especially on offshore oil and gas facilities.

Exemption requests are considered to ensure the approval of the request would not undermine the security of Australia's maritime transport system thereby increasing the risk of a terrorist act occurring.

Monitoring of cards issued

MSIC issuing bodies are required to develop and maintain MSIC plans which set out operating procedures in relation to the issue of MSICs. These plans are required to be approved by the Department before the issuing body can commence operations. The program must include procedures with regard to:

- the issue and production of MSICs.
- the safekeeping, secure transport and disposal of MSICs;
- the recovery and secure destruction of issued MSICs that are no longer required;
- lost, destroyed or stolen MSICs; and
- ensuring MSICs are returned to issuing bodies when they are no longer required.

An issuing body is required to keep a register of MSICs issued; the register must contain details of each MSIC issued by the body. These records are auditable by maritime security inspectors. Issuing bodies must provide annual reports to the Secretary at the end of each financial year outlining:

- the total number of MSICs issued by the body;
- the total number of MSICs issued by the body that have not expired and have not been cancelled;
- the number of MSICs issued by the body that have expired or been cancelled but have not been returned to the body;
- the number of MSICs issued by the body that were cancelled in the financial year to which the report relates; and
- the number of MSICs issued by the body that expired in that financial year.

Issuing bodies are subject to obligations with regard to cancellation of MSICs. An issuing body must cancel an MSIC if:

- the body finds out that the MSIC was not issued in accordance with the body's MSIC plan;
- the Secretary of the Department has notified the issuing body in writing that a security assessment of the holder was adverse; or

- the issuing body finds out that the holder has been convicted of a disqualifying offence.

Additionally, an issuing body must cancel an MSIC issued by the body if the holder of the MSIC asks the holder to cancel it. The issuing body must notify the Secretary of the Department of this cancellation.

There are also obligations on MSIC holders. The holder of an MSIC must return the MSIC to an issuing body 30 days or less after the MSIC expires, the card is cancelled, or the card is damaged altered or defaced. In addition, a holder is obligated to return an MSIC if he or she becomes aware of circumstances that will result in him or her not having an operational need to hold the MSIC for 12 months.

The obligations created for issuing bodies and MSIC holders ensure that cards are issued and held in a robust fashion and therefore do not compromise the broader purpose of the MSIC scheme which is to reduce the threat of a terrorist act occurring in the maritime transport system.

Temporary MSICs

The MTOFSR has provision to allow the issuing of temporary MSICs by maritime industry participants. A temporary MSIC can only be issued to a person if his or her card has been lost, destroyed, forgotten or has been stolen. In addition, a temporary card cannot be issued unless a security assessment of the applicant has been made and the Secretary is satisfied the applicant does not constitute a threat to the security of maritime transport or an offshore facility (in circumstances where no decision has yet been made about whether the person has an adverse criminal record). Temporary cards may also be issued where an MSIC has been approved but the applicant has yet to physically receive their MSIC.

Temporary MSICs are the responsibility of each maritime or offshore industry participant.

Conclusion

Efficient, safe and secure aviation and maritime transport systems are integral to Australia's economic well being. A terrorist attack would have catastrophic consequences, both economically and socially.

In a complex security environment, combined with an uncertain economic outlook, it is essential that OTS as regulator takes a pragmatic, practical approach to security regulation that balances the need for effective preventive security measures with the efficient facilitation of trade and passenger movements.

The need to strike this balance is reflected in the risk based approach OTS takes, which continuously enhances security in Australia's transport system. The preventive security measures required to be implemented by the aviation and maritime industries in accordance with the ATSA and MTOFSA are robust yet flexible enough to account for the varied operations conducted across the aviation and maritime transport sectors.

As OTS continues to mature as a regulator it will continue to build on the strong relationships it has with the aviation and maritime transport industries to ensure Australia is well placed to respond to new threats, reducing the likelihood that Australia's transport systems will a target of, or used for facilitating, a terrorist attack both now and into the future.