



Australian Government
Department of Home Affairs

Submission to the Inquiry into the Transport Security Amendment (Serious Crime) Bill 2019

Senate Legal and Constitutional Affairs Legislation Committee

Table of Contents

Department of Home Affairs' Submission	3
1. Introduction	3
2. The ASIC and MSIC Schemes	4
2.1. Background	4
2.1.1. ASICs and MSICs	4
2.1.2. Security-sensitive Areas	4
2.1.3. Background Checking	5
3. Transport Security Amendment (Serious Crime) Bill 2019	5
3.1. Purpose of Bill	5
3.2. Background on the Bill	6
3.3. Benefits of the Bill	6
3.4. Issues raised on the Bill	7
3.4.1. Security concerns	7
3.4.2. Penalties	7
3.4.3. Trusted insider threat	8
3.5. Consultation	8
4. Conclusion	8
Attachment A	9
Attachment B	10
Attachment C	12

Department of Home Affairs' Submission

1. Introduction

The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission to the Senate Legal and Constitutional Affairs Legislation Committee (the Committee) inquiry into the Transport Security Amendment (Serious Crime) Bill 2019 (the Bill) following its introduction into the House of Representatives on 23 October 2019.

Serious and organised crime is a major threat to the Australian way of life and causes enormous human suffering with highly visible flow-on effects to our community. Organised criminals are gaining a major source of revenue through the trafficking of illicit goods, such as drugs. In 2016-17, the Australian Institute of Criminology estimated the cost of serious and organised crime to be between \$23.8 billion to \$47.4 billion per annum¹. This cost will continue to rise and it is imperative that the Australian Government (the Government) puts measures in place to prevent serious and organised crime for the safety and security of all Australians.

Airports and seaports are transit points for organised crime groups to import weapons, illicit drugs and other harmful goods into Australia. This is a serious threat to Australia's security and prosperity. Securing Australia's airports, seaports and offshore facilities is vital to protect the Australian community and legitimate industries from terrorists and people with serious criminal convictions.

The aviation and maritime security identification card (ASIC and MSIC) schemes are an important part of securing the aviation, maritime and offshore facilities sectors. Several parliamentary and independent reviews² have identified vulnerabilities in the ASIC and MSIC schemes. In particular, the schemes vulnerability to exploitation by serious criminals and organised crime syndicates.

Notably, the Parliamentary Joint Committee on Law Enforcement (PJCLE), *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime* (2011) highlighted that the schemes were never originally designed to harden the transport environment against serious and organised crime. Organised crime groups have exploited gaps, weaknesses and inconsistencies in the application of the regimes. The National Ice Taskforce, *Final Report* (2015) also recommended that the Government should continue to protect the aviation and maritime environments against organised crime by strengthening the eligibility criteria for holders of ASICs and MSICs.

The Government is committed to reducing criminal influence at airports, seaports and offshore facilities and strengthening the ASIC and MSIC schemes to address serious crime. The passage of legislation currently before the House of Representatives will implement recommendations made by the PJCLE and the National Ice Taskforce. The legislation would also meet the Government's commitment to strengthen background checking regimes, ensuring that individuals with links to serious and organised crime cannot gain access to airports, ports and offshore facilities.

¹ Smith R 2018. *Estimating the costs of serious and organised crime in Australia 2016–17*. Statistical Reports no. 9. Canberra: Australian Institute of Criminology, at <https://aic.gov.au/publications/sr/sr09>.

² Australian National Audit Office Report, *The Management of the Aviation Security Identification Card and Maritime Security Identification Card Scheme* (2011); the Parliamentary Joint Committee on Law Enforcement (PJCLE), *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime* (2011) and the National Ice Taskforce, *Final Report* (2015).

2. The ASIC and MSIC Schemes

2.1. Background

The *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) establish the regulatory framework to safeguard against unlawful interference with aviation and maritime transport, and offshore facilities and meet Australia's international obligations. The ASIC and MSIC schemes are established under the *Aviation Transport Security Regulations 2005* (Aviation Regulations) and *Maritime Transport and Offshore Facilities Regulation 2003* (Maritime Regulations), prescribed under the ATSA and MTOFSA respectively, and are administered by the Department.

2.1.1. ASICs and MSICs

The ASIC and MSIC schemes are an important part of securing the aviation, maritime and offshore sectors and reducing the risk of terrorism. ASICs and MSICs are nationally consistent identification cards that show the holder has met the minimum security requirements to remain unmonitored within a secure area or security zone area at airports, seaports and offshore facilities respectively. As at 10 December 2019, there are approximately 148,727 validly issued ASICs and 105,503 validly issued MSICs.

To be eligible for an ASIC or MSIC, a person must have an operational need to access these secure areas and zones or work in a security sensitive position (e.g. screening officers, check-in staff, baggage handlers, stevedores, port and dock workers, truck drivers and seafarers on Australian regulated ships), and successfully pass a background check every two years.

If a person does not hold a valid ASIC or MSIC they must be escorted or supervised by an ASIC holder (in secure areas of an airport) or escorted or continuously monitored by an MSIC holder (in security zones of a seaport, Australian flagged ship or offshore oil and gas facility).

2.1.2. Security-sensitive Areas

Security-sensitive areas are discrete zones, defined as a 'secure area' in the Aviation Regulations and a 'maritime security zone' in the Maritime Regulations, established at airports, seaports and offshore facilities to protect critical or vulnerable aspects of our aviation and maritime infrastructure. Security-sensitive areas do not encompass entire airports or seaports. For example, the arrivals hall of an airport and the commodity storage area of a bulk loading terminal at a seaport are not defined as security-sensitive areas.

Security-sensitive areas are subject to stringent security measures, including access restrictions. Industry is responsible for controlling access to these areas, including ensuring that only a person who holds an ASIC or MSIC or a person escorted by an ASIC or MSIC holder may enter these areas. Security-sensitive areas include areas at:

- **security controlled airports**, such as the area immediately surrounding the regular public transport (RPT) aircraft apron; the runway and area around the runway; non-RPT aprons and hangars; aviation safety infrastructure; fuel storage areas; and areas encompassing air traffic control facilities and navigational aids; and

- **security regulated seaports**³, regulated Australian flagged ships and offshore facilities. These areas include parts of the dock/wharf and the water approaches to the berth; areas for screening passengers; waters surrounding the security regulated ship; the ship's engine room or bridge; waters surrounding the offshore facility; and the offshore facility's control room and production manifold.

2.1.3. Background Checking

AusCheck undertakes a background check for each individual who applies for an ASIC or MSIC. AusCheck sits in the Department and its functions are authorised under the *AusCheck Act 2007*.

The primary purpose of the background check for an ASIC or MSIC applicant is to establish whether an applicant may pose a threat to aviation and maritime security, or offshore facilities, such as a trusted insider (employee in a position to exploit a security system to conduct or enable an act of unlawful interference) who may have been radicalised.

A background check includes a national security assessment by the Australian Security Intelligence Organisation (ASIO), a criminal history check by the Australian Criminal Intelligence Commission (ACIC) to determine if an applicant has an unfavourable criminal history (such as an adverse criminal record) and, if required, an immigration check by the Department to assess the applicant's right to work. An applicant will have an adverse criminal record where they have been convicted and sentenced to a certain period of imprisonment for an aviation-security-relevant-offence (ASRO) or a maritime-security-relevant offence (MSRO) as defined by the Aviation and Maritime Regulations.

Under the ASIC and MSIC schemes, when an applicant has one or more ASROs or MSROs on their criminal record, there is a need to make an assessment to determine whether the applicant is eligible for a card. Currently, the schemes each have separate eligibility criteria which rely on inconsistent types of offences. These types of offences are designed to capture offences that are relevant for preventing unlawful interference (i.e. terrorist threats to aviation and maritime security) and do not consider whether the individual poses a serious criminal risk. Current ASIC (ASRO) and MSIC (MSRO) eligibility criteria are at **Attachment A and B**.

3. Transport Security Amendment (Serious Crime) Bill 2019

3.1. Purpose of Bill

Given the impact of serious and organised crime on the Australian community, the purpose of the Bill is to amend the ATSA and MTOFSA to reduce criminal influence at Australia's security controlled airports, security regulated seaports, and security regulated offshore facilities. Specifically, the Bill will:

- create an additional purpose in the ATSA and MTOFSA to prevent the use of aviation and maritime transport or offshore facilities in connection with serious crime;

³ Maritime security zones at seaports, unlike aviation security zones, are not always established on a full-time basis. However, MSICs are required at all times in a security zone. For example, the Port of Useless Loop in Western Australia has defined security zones that are switched on during a set period prior to a vessel berthing and switched off after a vessel departs. MSICs are only required in the security zone when the security zone is active.

- provide for the making of regulations for this additional purpose, which will provide for the strengthening of the eligibility criteria under the ASIC and MSIC schemes to target serious criminal offences;
- allow for regulations to be made for the additional purpose to prescribe penalties for offences against the regulations of up to 200 penalty units, consistent with penalty provisions across the ASIC and MSIC schemes;
- clarify and align the legislative basis for undertaking background checks of individuals under the ATSA and MTOFSA; and
- make technical amendments to improve the operation of the ATSA and MTOFSA.

3.2. Background on the Bill

The 2019 version of the Bill substantially replicates the Transport Security Amendment (Serious or Organised) Crime Bill 2016, which was introduced in the previous Parliament by the then Minister for Infrastructure and Transport (2016 Bill). The 2016 Bill did not pass prior to the dissolution of Parliament in April 2019.

The 2016 Bill was considered by the Senate Standing Committee for the Scrutiny of Bills (SCSB) and the Senate Standing Committee for Rural and Regional Affairs and Transport (RRAT), as the Bill previously sat within the Infrastructure and Transport Portfolio. The SCSB raised minor issues concerning the level of penalty able to be imposed by regulations, but did not raise any further issues. The majority report from RRAT recommended that the Bill be passed without amendment.

In comparison to the 2016 Bill, the 2019 Bill has been amended to capture new classes of ASICs and MSICs (white ASICs and white MSICs) that have been introduced into the Aviation and the Maritime Regulations. These amendments will ensure that all ASIC and MSIC applicants and holders will be captured by the new eligibility criteria. Some additional technical amendments are also included which align the regulation-making powers supporting the MSIC scheme in the MTOFSA with correlating powers supporting the ASIC scheme in the ATSA.

The 2019 Bill has been reconsidered by the SCSB and raised similar issues regarding the level of penalty imposed. SCSB has left the matter to the Senate for determination.

3.3. Benefits of the Bill

The amendments to the ATSA and MTOFSA which would be made by the Bill will establish the statutory framework required to introduce the proposed new eligibility criteria. This framework will address the existing vulnerability in the ASIC and MSIC schemes.

The current eligibility criteria do not provide for offences unrelated to unlawful interference with aviation and maritime security, and offshore facilities to be considered when assessing suitability to access security-sensitive areas. This has resulted in individuals with serious criminal histories, including convictions for involvement with a criminal organisation or gang and illegal importation of goods, being cleared to work at airports, seaports and offshore facilities. This restriction is caused by limitations in the ATSA and MTOFSA, which apply in turn to the ASIC and MSIC schemes. The amendments made by the Bill will allow for new, expanded, eligibility criteria to be prescribed in the Aviation and Maritime Regulations for the ASIC and MSIC schemes.

The proposed new eligibility criteria will target serious criminal offences. The new eligibility criteria will also be harmonised and apply a consistent approach to assessing risks in the aviation and maritime environment. Harmonising the criteria creates potential efficiencies where only a single criminal history checking process would be required for an ASIC and MSIC. The proposed new eligibility criteria are at **Attachment C**.

The proposed new eligibility criteria will introduce new types of offences such as offences relating to: anti-gang or criminal organisation legislation; illegal importation of goods; interfering with goods under customs control; and foreign incursion and recruitment. Commonwealth, State and Territory offences will be captured.

The proposed eligibility criteria will also introduce a tiered approach to types of offences. Under the current eligibility criteria, an ASIC or MSIC applicant's status is based solely on the presence of a relevant offence in the applicant's criminal history.

The tiers of the proposed new eligibility criteria comprise:

- **Tier 1** contains disqualifying offences (such as terrorism). Persons convicted of Tier 1 offences will be disqualified from being issued an ASIC or MSIC and will not have access to a discretionary assessment.⁴ These persons will continue to have access to appeal the decision by application to the Australian Government's Administrative Appeals Tribunal (AAT).
- **Tiers 2-5** contain offences that would result in an adverse criminal record and the person being unable to be issued an ASIC or MSIC following the initial application. These persons may be eligible for an ASIC or MSIC under a discretionary process that is already established under the Aviation and Maritime Regulations (see reg 6.29 and reg 6.08F respectively). Discretionary assessments are also subject to AAT review.

All existing appeals processes will remain available for ASIC and MSIC applicants under the proposed new eligibility criteria. Applicants denied an ASIC or MSIC will continue to have the option to seek a discretionary assessment, unless they have been convicted of a Tier 1 offence, or appeal the decision to the AAT.

3.4. Issues raised on the Bill

3.4.1. Security concerns

Some concerns were previously raised that the Bill will make Australia's transport security less secure by introducing the new purpose of preventing the use of aviation and maritime transport or offshore facilities in connection with serious crime in the ATSA and MTOFSA, taking focus from counter-terrorism. The introduction of an additional purpose does not reduce the effectiveness of the counter-terrorism aspects of the ASIC and MSIC schemes.

Reforms to the eligibility criteria for the ASIC and MSIC schemes will not affect the fundamental integrity of security assessments, as a national security assessment will remain as a component of a background check and is not dependant on the presence of a conviction in an applicant's criminal history. In practice, the process for assessing national security outcomes will not change and will continue to be undertaken by ASIO under the *Australian Security Intelligence Organisation Act 1979*, which is not being amended by the Bill. Further, the ability to consider offences such as foreign incursion and recruitment in the proposed new eligibility criteria will enhance the schemes' ability to exclude persons convicted of offences of the highest severity and that may be closely linked to terrorist activity, but not directly related to unlawful interference with aviation and maritime transport.

3.4.2. Penalties

The SCSB has raised concerns that the maximum penalty that could be prescribed by regulations made under the Bill may be up to 200 penalty units which is above what is recommended by the *Commonwealth*

⁴ The Aviation and Maritime Regulations enable the Secretary of the Department to undertake a discretionary assessment to approve the issue of an ASIC or MSIC to applicants who have an adverse criminal history record. The discretionary assessment includes a comprehensive review of the applicant's individual circumstances.

Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers (Commonwealth Guide).

The Department considers that the proposed penalties are an appropriate deterrence mechanism given the security-sensitive environment at airports, seaports and offshore facilities which may be targeted by criminal enterprises to facilitate the movement of illicit goods.

The 200 penalty unit maximum penalty threshold does not apply to the public at large, it only applies to offences committed by an 'airport operator or aircraft operator' as defined by the ATSA or a 'port operator, ship operator, port facility operator or offshore facility operator' as defined by the MTOFSA. A 100 penalty unit maximum penalty threshold only applies to offences committed by 'an aviation industry participant' or a 'maritime industry participant' subject to limited exceptions.

The Commonwealth Guide also states that penalties prescribed by legislation should be consistent with penalties prescribed for existing offences of a similar kind or of a similar seriousness. The provisions in the Bill align with other regulation-making provisions under the ATSA and MTOFSA. This advice was given primary consideration during the course of drafting the Bill.

In addition, nothing in the proposed provisions requires offences to be prescribed with a maximum penalty greater than 50 penalty units. The Bill only provides a discretion for greater penalties to be prescribed. Appropriate consideration will be given to the penalty thresholds for regulations made under the proposed provisions and, if required to be above the general 50 penalty unit threshold, appropriate justification would be provided in explanatory materials.

3.4.3. Trusted insider threat

Some stakeholders raised concerns that the Bill does not address a trusted insider's ability to infiltrate Australia's transport security sector. The Bill facilitates changes to the ASIC and MSIC eligibility criteria which will have the practical consequences of ensuring individuals with serious criminal records that pose a criminal risk, will not lawfully be able to access security-sensitive areas, unless escorted by a valid cardholder. This is likely to result in the removal of some individuals that pose a trusted insider risk.

3.5. Consultation

Stakeholder consultation across the aviation and maritime sectors was undertaken during the development of the Bill. Consultation began in August 2011, immediately following the release of the PJCLE's final report in June 2011. This included a range of discussion papers as well as presentations and agenda items at various industry forums, which included participants from the aviation and maritime sectors.

In addition, consultation was undertaken with relevant government agencies including the ACIC, Australian Federal Police, ASIO and State and Territory police and justice agencies.

4. Conclusion

An efficient, safe and secure transport system is integral to Australia's social and economic well-being. The Department takes an active approach to transport security regulation, reflecting on what Government knows about security threats to ensure that Australia's transport security system is fit for purpose and security measures are targeted to areas of highest risk.

The amendments that would be made by the Bill will strengthen the schemes to prevent individuals that are a high criminal risk from holding a card, ensuring that Australia's security controlled airports, security regulated seaports and security regulated offshore oil and gas facilities are secure.

ATTACHMENT A

Current ASIC eligibility criteria (aviation-security-relevant offences)

Regulation 6.01 of the *Aviation Transport Security Regulations 2005*

	Item	Kind of offence
A person is initially ineligible for an ASIC where they have been convicted of an aviation-security-relevant offence (ASRO) and sentenced to imprisonment, or a person has been convicted twice or more of an ASRO (with one of those convictions within 12 months ending on the date when the relevant background check was conducted) but no sentence of imprisonment was imposed. However a person with an offence in this category may apply for a discretionary card and seek review through the Administrative Appeals Tribunal.	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: <ul style="list-style-type: none"> a) a narcotic substance within the meaning of the <i>Customs Act 1901</i>; or b) a drug, within the meaning of: <ul style="list-style-type: none"> i. Regulation 10 of the <i>Customs (Prohibited Exports) Regulations 1958</i>; or ii. Regulation 5 of the <i>Customs (Prohibited Imports) Regulations 1956</i>
	5	An offence, of a kind dealt with in Part II of the <i>Crimes Act 1914</i> , against the Government of: <ul style="list-style-type: none"> 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 <i>Crimes (Aviation) Act 1991</i>
	7	An offence against Part 5.3 of the <i>Criminal Code</i>
	8	An offence constituted by the production, possession, supply, import or export of explosives or explosive devices.

ATTACHMENT B

Current MSIC eligibility criteria (maritime-security-relevant offences)

Schedule 1 of the *Maritime Transport and Offshore Facilities Security Regulations 2003*

	Item	Kind of offence
<p>Part 1. Disqualifying offences: A person convicted of an offence mentioned in Part 1 is disqualified from holding a MSIC and cannot apply for a discretionary card.</p> <p>The person may seek reconsideration through the Administrative Appeals Tribunal.</p>	1.1	terrorism
	1.2	treason, sedition, espionage or selling national secret
	1.3	weapon of mass destruction
	1.4	hijacking or destruction of an aircraft, vessel or offshore facility
<p>Part 2. A person is initially ineligible for a MSIC where they have been convicted of an offence mentioned in Part 2, and sentenced to imprisonment for that offence. However a person with an offence in this category may apply for a discretionary card.</p>	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: <ul style="list-style-type: none"> • grievous bodily harm • actual bodily harm • torture • wounding • aggravated sexual assault • assault with use of weapon • assault in company
	2.9	kidnap
	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
	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.

ATTACHMENT C

Proposed ASIC and MSIC eligibility criteria

1.	Tier 1: Disqualifying Offences (Person convicted of an offence)
1.1	Terrorism
1.2	Treason, sedition, espionage or selling national secrets
1.3	Engagement in hostile activities in a foreign country or involvement with foreign armed forces
1.4	Weapons of mass destruction
1.5	Hijacking or destruction of a government or commercial aircraft, vessel or offshore facility
1.6	Endangering a government or commercial aircraft, airport, vessel, port or offshore facility
1.7	Piracy at sea
1.8	An offence relating to involvement with a criminal organisation or gang
1.9	Smuggling or trafficking of people
2.	Tier 2: Offences for which conviction is adverse
2.1	Threatening or assaulting persons in or on an aircraft, airport, vessel, port or offshore facility
2.2	Theft of a government or commercial aircraft or vessel
2.3	An offence relating to questioning conduct by a person or body investigating serious crime or corruption
2.4	An offence under the <i>Aviation Transport Security Act 2004</i> that is punishable by imprisonment (whether or not the person is in fact sentenced to imprisonment)
2.5	An offence under the <i>Maritime Transport and Offshore Facilities Security Act 2003</i> that is punishable by imprisonment (whether or not the person is in fact sentenced to imprisonment)
3.	Tier 3: Offences for which a sentence of imprisonment is adverse
3.1	Murder and manslaughter
3.2	An offence relating to firearms, ammunition, weapons or use of items as a weapon
3.3	An offence relating to explosives or explosive devices
3.4	Production, possession, supply, importation or exportation of an illegal drug or controlled substance
3.5	Illegal importation or exportation of goods, fauna or flora
3.6	Bribery or corruption
3.7	Perjury or otherwise relating to perversion of the course of justice
3.8	An offence relating to use of a false identity or identity documents
3.9	An offence relating to interference with goods under Customs control
3.10	Unauthorised use, access, modification or destruction of data or electronic communications
4.	Tier 4: Offences for which a sentence of imprisonment is adverse
4.1	Hostage-taking, deprivation of liberty or false imprisonment
4.2	Racial hatred or racial vilification
4.3	Assaulting or resisting a law enforcement officer or other public officer
4.4	Impersonation of a law enforcement officer or other public officer
4.5	Extortion or blackmail
4.6	Dealing with proceeds of crime
4.7	Currency violations and money laundering
4.8	Arson
5.	Tier 5: Offences for which a sentence of imprisonment is adverse
5.1	Theft (other than offences referred to in tiers 1 to 4)
5.2	Forgery or fraud
5.3	Offences involving the sexual abuse or exploitation of a child
5.4	Assaultive offences, including indecent or sexual assaults (other than offences referred to in tiers 1 to 4)
5.5	Offences relating to intimidation (other than offences referred to in tiers 1 to 4)
5.6	Offences relating to endangerment of others (other than offences referred to in tiers 1 to 4), but not including traffic offences except where a vehicle is used as a weapon
5.7	Affray or riot
5.8	Tax evasion