

## **Chapter 5**

### **Aviation Security Identification Cards (ASIC) and Visitor Identification Cards (VIC)**

5.1 ASICs provide access to secure areas of airports. They are issued to employees who have cleared required background checks and who require frequent access to these secure areas. A VIC must also be worn in secure airport areas, but are issued to temporary or non-frequent airport visitors for a maximum of 28 days in a year.

5.2 The committee recognises that there have been a number of reviews into the ASIC scheme over recent years, resulting in ongoing reforms and amendments to the program. These reviews are considered in this chapter. The chapter also discusses legislative changes currently before the Senate which seek to amend ASIC eligibility and address security risks.

5.3 During the inquiry, a number of concerns were raised about the misuse of ASICs and VICs and the impact of such activity on aviation and airport security. This chapter details these concerns and the security risks they present.

#### **Background**

##### *Aviation Security Identification Cards*

5.4 The ASIC scheme seeks to ensure that individuals employed in or regularly accessing secure or 'sterile areas' in the aviation sector are subject to a certain level of background checking. Since its inception, the scheme has been subject to a number of changes. While initially applicants were only subject to criminal record checks, following the September 11 terrorist attacks, the scheme was expanded to cover a greater number of airports and airport staff. It was also strengthened through the introduction of tighter criminal history checks and an Australian Security Intelligence Organisation (ASIO) security assessment.

5.5 The ASIC scheme is provided for in the Regulations and is administered by the department.

##### *ASIC processing*

5.6 ASICs identify a person who has undergone a background check. According to the department, it shows that the person has met the minimum security requirements to access secure areas of a security controlled airport. However, the

ASIC is not an access card, as the relevant authority at each airport controls access to its secure areas.<sup>1</sup>

5.7 In 2016, the department informed the Senate Rural and Regional Affairs and Transport Legislation Committee (legislation committee) that as of 31 March 2016, 138 825 valid ASICs were in use, with an average of 119 300 ASIC/MSIC applications annually processed since 2010 (when reapplication every two years was introduced).<sup>2</sup>

5.8 Applicants for an ASIC need to apply to an ASIC issuing body. ASICs are not issued by a government agency; this task instead lies with a number of private and public sector issuing bodies, appointed under the Act. They include airport operators, airlines, aviation organisations, and commercial ASIC service providers.<sup>3</sup> As of March 2017, there were 44 different issuing bodies.<sup>4</sup>

5.9 Under current arrangements, ASIC background checking is conducted by the Australian Background Checking Service (AusCheck) on behalf of an issuing body. AusCheck coordinates vetting arrangements that underpin the ASIC scheme. Vetting includes:

- a criminal record check by CrimTrac, used to determine if an applicant has an adverse criminal record;
- a security assessment by ASIO; and
- if required, a right to work check by the Department of Immigration and Border Protection.<sup>5</sup>

5.10 An ASIC may be refused if an applicant returns an adverse criminal history check, or, if already issued, may be cancelled due to an adverse criminal record. Applicants have legal rights for reconsideration or appeal if denied an ASIC. In certain circumstances, applicants with an adverse criminal record can apply for department consideration, based on their individual circumstances. If successful, they will receive a discretionary ASIC card. An adverse criminal record includes:

---

1 Department of Infrastructure and Regional Development, *Aviation security identification*, October 2016, [https://infrastructure.gov.au/security/identity/aviation-security-information/index.aspx#anc\\_asic](https://infrastructure.gov.au/security/identity/aviation-security-information/index.aspx#anc_asic) (accessed 20 January 2017).

2 Senate Rural and Regional Affairs and Transport Legislation Committee, *Transport Security Amendment (Serious or Organised Crime) Bill 2016 [Provisions]*, April 2016, p. 2.

3 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, p. 118.

4 A list of issuing bodies is available at: <https://infrastructure.gov.au/security/identity/aviation-security-information/asic-issuing-bodies.aspx>.

5 Department of Infrastructure and Regional Development, *Applying for an aviation security identification card (ASIC)*, November 2016, <https://infrastructure.gov.au/security/identity/aviation-security-information/applying-for-an-asic.aspx> (accessed 23 January 2017).

- an aviation-security-relevant offence and sentenced 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.<sup>6</sup>

5.11 The current regulations define an aviation-security-relevant offence as 'an offence of a kind mentioned in the following table against a law of the Commonwealth, or of a State or Territory, or of any other country or part of a country'.<sup>7</sup>

**Table 5.1: Aviation security-relevant offences**

Item	Kind of offence
1	An offence involving dishonesty
2	An offence involving violence or a threat of violence
3	An offence involving intentional damage to property or a threat of damage to property
4	An offence constituted by the production, possession, supply, import or export of a substance that is: <ul style="list-style-type: none"> <li>(a) a narcotic substance within the meaning of the Customs Act 1901; or</li> <li>(b) a drug, within the meaning of: <ul style="list-style-type: none"> <li>(i) regulation 10 of the Customs (Prohibited Exports) Regulations 1958; or</li> <li>(ii) regulation 5 of the Customs (Prohibited Imports) Regulations 1956</li> </ul> </li> </ul>
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"> <li>(a) the Commonwealth or a State or Territory; or</li> <li>(b) a country or part of a country other than Australia</li> </ul>
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

5.12 The Regulations specify three types of ASIC security passes which permit access to security zones:

- ASIC— issued for those who require access to 'secure areas';
- temporary ASIC—issued the ASIC holders when an ASIC is lost, stolen or destroyed; and

6 Department of Infrastructure and Regional Development, *Applying for an aviation security identification card (ASIC)*, 10 February 2017, <https://infrastructure.gov.au/security/identity/aviation-security-information/applying-for-an-asic.aspx> (accessed 2 March 2017) and *Discretionary aviation security identification cards (ASICS): Frequently asked questions*, 11 December 2015, <https://infrastructure.gov.au/security/identity/aviation-security-information/faq-asic.aspx> (accessed 2 March 2017)

7 Aviation Transport Security Regulations 2005, s. 6.01.

- visitor identification cards (VICs)—issued to people needing to visit a secure area who are supervised by the holder of a valid ASIC while in the area.<sup>8</sup>

## Reforms to ASIC

5.13 As with aviation security regulation more generally, the ASIC scheme has been subject to ongoing reviews and amendments. While this has led to improvements in the scheme's administration, the committee was directed by the evidence to numerous areas that could be enhanced to improve security outcomes.

### *Wheeler Review 2005*

5.14 The Wheeler Review found a number of weaknesses within the ASIC system as well as 'confusion as to what airport access an ASIC enables'. Wheeler found that the criminal checking regime relied on convictions in a database at a point in time from the issuance of a two-year card. As subsequent recorded convictions were not automatically registered after a background check was completed, applicants with a pattern of criminality or with major criminal associations could still potentially be given access. Furthermore, Wheeler found that:

- the checking process could take weeks to complete, causing 'unacceptable reliance on procedures for visitor cards which do not require background checks';
- there were 188 ASIC databases and authorising bodies around Australia that were neither consistent nor linked; and
- some casual or contract workers, such as security screeners or cleaners didn't initially hold ASICs and were not necessarily always accompanied on-the-job by an ASIC holder as required under the legislation.<sup>9</sup>

5.15 Wheeler recommended that the background checking process required in obtaining and holding an ASIC be further tightened and centralised in the Attorney-General's Department (AGD) and that this should be harmonised with maritime cards.<sup>10</sup> AusCheck, operating on a cost-recovery basis, now performs background security checks for ASIC applications in line with the Wheeler Review recommendations, thus 'improving consistency and robustness of checking'.<sup>11</sup>

---

8 Aviation Transport Security Regulations 2005, part 6, ss. 6.03, 6.36 and 6.38.

9 Rt. Hon Sir John Wheeler, *An Independent Review of Airport Security and Policing for the Government of Australia*, Australian Government, September 2005, p. xiii.

10 Rt. Hon Sir John Wheeler, *An Independent Review of Airport Security and Policing for the Government of Australia*, Australian Government, September 2005, Recommendation X, p. xix.

11 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, p. 118.

---

### ***Aviation White Paper 2009***

5.16 The National Aviation Policy White Paper was published in December 2009. It contained a series of measures directed at strengthening aviation security including the ASIC regime. These measures include:

- strengthening the cancellation provisions for ASIC governing bodies and increasing penalties for false declarations by applicants;
- allowing for subsequent background checks for ASIC holders where their eligibility may have changed; and
- tightening visitor management provisions at security controlled airports.<sup>12</sup>

5.17 The white paper advocated for administrative changes to streamline the ASIC scheme, including a reduction in the number of issuing bodies, and providing that ASIC cards display a specified expiry date, rather than a specified month.<sup>13</sup>

### ***ANAO audit 2011***

5.18 In May 2011, the ANAO tabled a performance audit of the ASIC and Maritime Security Identification Card (MSIC) schemes. The ANAO made three recommendations regarding governance arrangements, issuing processes, and information management. All three recommendations were directed towards the OTS.

5.19 The ANAO recommended that OTS:

- review the risks arising from the administrative practices of issuing bodies, particularly in the issuing and manufacture of cards, and evidence of the confirmation of an applicant's identity. The outcomes of this review were to assess whether arrangements provided an appropriate level of assurance that the scheme's requirements were being met;
- increase the use of information obtained from its audit, inspection and stakeholder program to focus further compliance activities on areas that represented the greatest security risk; and
- monitor the actual usage of VICs at security-controlled airports and use this information to inform ongoing development of the ASIC scheme.<sup>14</sup>

---

12 Department of Infrastructure, Transport, Regional Development and Local Government, *National aviation policy white paper: flight path to the future*, Aviation White Paper, 2009, p. 22

13 Department of Infrastructure, Transport, Regional Development and Local Government, *National aviation policy white paper: flight path to the future*, Aviation White Paper, 2009, p. 143.

14 Australian National Audit Office, *Performance Audit Report No. 39 2010–11, Management of the Aviation and Maritime Security Identification Card Schemes*, pp. 24-25.

## **PJCLE 2011**

5.20 Under its terms of reference for its 2011 inquiry, the PJCLE examined the effectiveness of the ASIC and MSIC schemes. It considered how these cards were issued, monitored and stored, and how information was shared between appropriate law enforcement agencies.<sup>15</sup>

5.21 The PJCLE expressed its concern about the significant risk posed by criminal infiltration of the aviation workforce. As a means of preventing such infiltration, the PJCLE recommended that the AGD review the list of relevant security offences under the ASIC scheme. This review would assess whether any further offences were required to effectively extend those schemes to protect the aviation sector against the threat of infiltration by serious and organised criminal networks.<sup>16</sup>

5.22 The government agreed to this recommendation and undertook to 'review the lists of security-relevant to assess whether any further offences are required'.<sup>17</sup>

5.23 A further recommendation called for the harmonisation of the MSIC and ASIC eligibility criteria. The government agreed to review the ASIC and MSIC eligibility exclusion criteria to seek greater harmonisation, where appropriate.<sup>18</sup>

## **National Ice Taskforce 2015**

5.24 The 2015 final report of the National Ice Taskforce noted that ASIC and MSIC background checks did not consider criminal intelligence. It argued that 'the use of criminal intelligence in the background checking process for ASIC and MSICs could help identify links to organised crime among workers'.<sup>19</sup> The report recommended:

The Commonwealth Government should continue to protect the aviation and maritime environments against organised crime by strengthening the eligibility criteria for holders of Aviation Security Identification Cards and Maritime Security Identification Cards; and establishing a legal mechanism

---

15 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, June 2011, pp. 1-2.

16 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, Recommendation 14, June 2011, p. 93.

17 Government Response to the Report of the Parliamentary Joint Committee on Law Enforcement: *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, September 2011, p. 11.

18 Government Response to the Report of the Parliamentary Joint Committee on Law Enforcement: *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, September 2011, p. 12.

19 Prime Minister and Cabinet, *Final Report of the National Ice Taskforce*, 2015, p. 139.

---

to enable compelling criminal intelligence to be used in determining suitability of workers to hold such a card.<sup>20</sup>

### *Other reforms*

5.25 According to the department, a range of improvements to the ASIC scheme are underway. Stage one commenced on 1 November 2016 and stage two will commence on 1 August 2017.<sup>21</sup>

5.26 A white, role-specific ASIC was introduced from 1 November 2016, and is issued to individuals who require a valid background check, but not access to airport secure areas (for example, an employee of an organisation that issues ASICs and VICs).<sup>22</sup>

5.27 In addition, from 1 November 2016, issuing bodies have been required to include greater procedural content in ASIC programs and MSIC plans, and a background check is required of all applicants under 18 years of age. From 1 August 2017, applicants will need to be verified via face-to-face meetings, and new categories of identification will be introduced.<sup>23</sup>

### **Transport Security Amendment (Serious or Organised Crime) Bill 2016**

5.28 The ASIC scheme was introduced through national security aviation legislation to protect the aviation workforce from infiltration by terrorist organisations. It was not designed to specifically target criminality and organised crime.<sup>24</sup> However, the various reviews into the ASIC scheme, as detailed above, have also argued for more stringent background and criminal checks.

5.29 Law enforcement agencies and others have argued that the purpose of the ASIC scheme could be broadened to provide general crime prevention measures.<sup>25</sup> For example, the IBPP was supportive of changes to the ASIC scheme to address a

---

20 Prime Minister and Cabinet, *Final Report of the National Ice Taskforce*, 2015, p. 139.

21 Department of Infrastructure and Regional Development, *Identity security amendments*, October 2016, <https://infrastructure.gov.au/security/identity/Identity-security-regulatory-amendments.aspx>

22 Department of Infrastructure and Regional Development, *ASIC issuing body – Role-specific white ASIC*, Factsheet 2 – Identity Security Amendments, 1 November 2016, [https://infrastructure.gov.au/security/files/ASIC\\_issuing\\_body-Role-specific\\_white\\_ASIC.pdf](https://infrastructure.gov.au/security/files/ASIC_issuing_body-Role-specific_white_ASIC.pdf) (accessed 20 January 2017).

23 Department of Infrastructure and Regional Development, *Identity security amendments*, October 2016, <https://infrastructure.gov.au/security/identity/Identity-security-regulatory-amendments.aspx>

24 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the Adequacy of Aviation and Maritime Security Measures to Combat Serious and Organised Crime*, June 2011, p. 83.

25 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, p. 117.

range of criminal threats and vulnerabilities, and 'to enhance the ability of the schemes to support broader law enforcement purposes, including for national security purposes'.<sup>26</sup>

5.30 The Transport Security Amendment (Serious or Organised Crime) Bill 2016 (transport security bill) is currently before the Senate and seeks to address a number of security concerns, and in particular responds to ASIC recommendations made by the PJCLE in 2011. The Minister for Infrastructure and Transport, the Hon Darren Chester MP, noted that the bill addressed the current lack in the ASIC scheme of a check for criminal risk.<sup>27</sup>

5.31 The transport security bill seeks to harmonise the ASIC and MSIC eligibility criteria, to streamline the application process and reduce waiting times (thus addressing some concerns raised in the Wheeler Review). The bill introduces a new 'tier' approach to the eligibility criteria to better target serious or organised crime, such as:

- offences under anti-criminal organisation legislation;
- the illegal sale and possession of firearms and other weapons; and
- illegal importation of goods and interfering with goods under Border Force control.<sup>28</sup>

5.32 The eligibility criteria will be broken into 5 tiers. Tier 1 contains all 'disqualifying' offences, and anyone with such an offence will be disqualified from obtaining an ASIC. Examples include terrorism, hijacking or destroying an aircraft, and an offence related to involvement with a criminal organisation or gang. Tiers 2 to 5 are 'adverse' offenses that:

contain offences that would result in a person being found to have an adverse criminal record and unable to be issued with an ASIC/MSIC following the initial application. These persons will be eligible to apply for an ASIC/MSIC through the discretionary assessment.<sup>29</sup>

5.33 In effect, less serious offences will require 'a higher imprisonment threshold to become an aviation or maritime-security-relevant offence, while more serious offences will only require conviction'. Examples of offences in these tiers include

---

26 Immigration and Border Protection Portfolio, *Submission 19*, p. 6.

27 The Hon Darren Chester MP, Airport security oped, 'Tougher border worker checks needed', *Daily Telegraph*, 1 March 2017, [http://minister.infrastructure.gov.au/chester/opinion/2017/dco\\_002\\_2017.aspx](http://minister.infrastructure.gov.au/chester/opinion/2017/dco_002_2017.aspx) (accessed 2 March 2017).

28 Department of Infrastructure and Regional Development, *Proposed new eligibility criteria for the ASIC and MSIC schemes*, 14 February 2017, <https://infrastructure.gov.au/security/news/20160211-asic-msic.aspx> (accessed 2 March 2017).

29 Department of Infrastructure and Regional Development, *Proposed new eligibility criteria for the ASIC and MSIC schemes*, 14 February 2017.



---

assault of a person on an aircraft, illegal import of goods, bribery, corruption, blackmail, dealing with proceeds of crime, and forgery or fraud.<sup>30</sup>

5.34 The committee noted the previous work of the legislation committee in the 44<sup>th</sup> Parliament which examined the transport security bill, and the concerns raised about the targeting of serious crime via transport security legislation:

Transport security is a vital mission for government – but it is a qualitatively different task from targeting organised crime in our transport system...There is potential risk that widening the purpose of transport security legislation will confuse the two missions of transport security and targeting serious or organised crime in the transport system. Both these tasks are important – the question is whether achievement of both is best done via the mechanisms [in this bill].<sup>31</sup>

5.35 In responding to the legislation committee's report, the government noted that the transport security bill does not affect the national security assessment component of ASIO background checks. It also argued against a new security regime, noting that:

extending the current ASIC and MSIC regimes is more efficient and effective than developing a new and separate scheme to counter serious or organised crime at our airports and ports.

The existing ASIC and MSIC schemes are well understood by industry. Introducing a new scheme would likely impose additional costs and lead to confusion and inadvertent non-compliance.<sup>32</sup>

5.36 Given the evidence before it, the legislation committee supported the introduction of a more rigorous background checking regime, and excluding potential security risks from accessing important aviation infrastructure. The legislation committee supported having harmonised eligibility criteria across both security card schemes.

5.37 The amendments reflect the position reached by a number of previous reviews into the ASIC scheme. A number of administrative concerns with the ASIC scheme were not within the scope of the transport security bill.

---

30 Department of Infrastructure and Regional Development, *Proposed new eligibility criteria for the ASIC and MSIC schemes*, 14 February 2017.

31 Senate Rural and Regional Affairs and Transport Legislation Committee, *Transport Security Amendment (Serious or Organised Crime) Bill 2016 [Provisions]*, Additional comments, April 2016, p. 15.

32 Australian Government response to the Senate Rural and Regional Affairs and Transport Legislation Committee report: *The Transport Security Amendment (Serious or Organised Crime) Bill 2016*, p. 3.

### ***Self-reporting concerns***

5.38 Under the current Regulations, there are self-reporting obligations for ASIC card holders. An ASIC card holder, who is convicted of and sentenced for an aviation-security-relevant offence, must report this to the ASIC issuing body or the Secretary of the AGD, within seven days. It is an offence not to do so. The issuing body or AusCheck will then complete another background check. If the background check returns an adverse or disqualifying result, the ASIC is cancelled and the card must be returned.<sup>33</sup>

5.39 The transport security bill makes no changes to this self-reporting regime. Under the revised ASIC eligibility criteria it will continue to be an offence for a card holder to not report a conviction and sentence to an issuing body.<sup>34</sup>

5.40 ASIAL argued that the two-year validity of cards, in conjunction with the absence of an automatic notification system for convictions of relevant offences, could compromise airport and aviation security. ASIAL suggested the introduction of a constant monitoring program for criminal activity that would identify aviation workers no longer suitable for work in secure areas of airports.<sup>35</sup>

5.41 The PJCLE, in its 2011 report, recommended that AusCheck and CrimTrac work together to establish mechanisms for continual assessment of a card holder's criminal record. This would allow disqualification of an ASIC very soon after a conviction, rather than waiting for the conviction to become apparent during a two-year renewal background check.<sup>36</sup>

5.42 In its response to the PJCLE report, the government noted the recommendation and endeavoured to work with other agencies to 'explore options' in this area. It noted, however, that 'there are a number of technical, privacy, legislative and funding issues that need to be resolved to achieve this outcome'.<sup>37</sup>

5.43 The department stated that it was not feasible to implement a continuous background-checking system with automatic notifications, due to the limitations of current technology and data-sharing between a range of federal and state agencies. Ms Sachi Wimmer, OTS, explained:

---

33 Aviation Transport Security Regulations 2005, s. 6.41.

34 Department of Infrastructure and Regional Development, *Proposed new eligibility criteria for the ASIC and MSIC schemes*, 14 February 2017, <https://infrastructure.gov.au/security/news/20160211-asic-msic.aspx> (accessed 2 March 2017).

35 Australian Security Industry Association Limited, *Submission 13*, p. 4.

36 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, June 2011, pp. 105-106.

37 Government Response to the Report of the Parliamentary Joint Committee on Law Enforcement: *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, September 2011, p. 13.

At the moment it is not possible to [create a continuous background checking system]. We are not responsible for it. It is actually the Attorney-General's Department that undertakes all the background checking for us for the ASIC scheme, through their centralised background-checking unit, AusCheck.

...there are significant challenges in developing a system, even in this age of technology, that is a continuous background-checking system, because it actually requires all of the police forces in Australia to come together with the same system, the same processes.<sup>38</sup>

5.44 ASIO declined to comment on whether the lack of an automated system could seriously compromise aviation security. However, it noted the organisation would welcome an automatic notification system, should it be possible:

...we would certainly welcome that. I have no idea about systems development and how easy that is to do, but obviously we rely on information flow coming through....Particularly for us, if it is of a national security concern—from the AFP and in criminal matters—I am sure that the sooner we can get that, the better.<sup>39</sup>

### *Shortcomings of the ASIC*

5.45 The committee received some evidence that the ASIC scheme, while strongly regulated in parts, was open to some abuse. For example, as part of the Seven Network's 2014 investigations, an ex-employee claimed that after their resignation, they were able to use their ASIC card to access secure airport areas '50 times'.<sup>40</sup>

5.46 In relation to ASIC holders, Mr Allan Kessing argued that airport ground staff issued with an ASIC were not subject to vigorous background checking. He further noted that the 2003 report into aviation security at Sydney Airport found that:

Twenty per cent of persons holding those identification cards enabling access to the sterile areas were found to have criminal convictions, and about half of those were serious convictions, including drug trafficking, assault and other misdemeanours.<sup>41</sup>

5.47 Much to the concern of the committee, Mr Kessing went on to state that:

What was most worrying was the degree of identity fraud in obtaining [ASIC] cards. There were a number of individuals who had cards in multiple names. There were at least eight people who were unidentifiable

---

38 Ms Sachi Wimmer, Office of Transport Security, Department of Infrastructure and Regional Development, *Committee Hansard*, 6 February 2015, p. 64.

39 Ms Kerri Hartland, Australian Security Intelligence Organisation, *Committee Hansard*, 6 February 2015, p. 59.

40 Mr Bryan Seymour, *Submission 1*, p. 11.

41 Mr Allan Kessing, *Submission 21*, p. 4; Mr Allan Kessing, private capacity, *Committee Hansard*, 24 November 2016, p. 3.

by any known database. They did not exist. They were not on the electoral roll. They did not have drivers licences. They did not own cars.<sup>42</sup>

5.48 The Wheeler Review identified that some workers who were yet to receive their initial ASIC card were not accompanied in airport secure areas by ASIC card holders, as required by law. Workers without a valid ASIC included cleaners and security screeners.<sup>43</sup>

5.49 Submissions to the 2014 ASRR argued that ASICs were a significant regulatory burden with issues surrounding expense, renewal frequency, and duplication with other forms of identification, particularly for pilots.<sup>44</sup>

5.50 Specifically, concerns were raised about ASICs in relation to:

- disproportionate expenses for smaller operators;
- the two-year renewal requirement being excessive and inflexible;
- scepticism about the actual benefits received by pilots, owners and operators; and
- duplication with other valid forms of identification, such as pilot licences.<sup>45</sup>

5.51 In its final report, the ASRR found that:

...submissions questioned the validity of the ASIC requirements, in particular for operators at regional and remote airports where it was noted that other security measures such as perimeter fencing and passenger screening are sometimes minimal and the ASIC regime is seen by industry as disproportionate to the level of localised risk. Submissions suggested that ASICs create a significant impost without delivering a commensurate security benefit.<sup>46</sup>

5.52 The ASRR made numerous recommendations, including amending the Regulations so that background checks and the requirement to hold an ASIC card

---

42 Mr Allan Kessing, private capacity, *Committee Hansard*, 24 November 2016, p. 3.

43 Rt. Hon Sir John Wheeler, *An Independent Review of Airport Security and Policing for the Government of Australia*, Australian Government, September 2005, p. xiii.

44 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, [https://infrastructure.gov.au/aviation/asrr/files/ASRR\\_Report\\_May\\_2014.pdf](https://infrastructure.gov.au/aviation/asrr/files/ASRR_Report_May_2014.pdf), p. 119.

45 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, p. 119. See also Mr Richard Rudd, *Submission 7*, p. 1.

46 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, p. 119.

would only be required for unescorted access to SRAs, not for general airside access.<sup>47</sup>

## Visitor Identification Cards

5.53 VICs are issued to individuals who are not required to have ASICs but have a lawful reason to temporarily or infrequently enter the secure zones of a security-controlled airport.<sup>48</sup> No background check is required to obtain a VIC.

5.54 Individuals issued with VICs are required to remain under the direct supervision of an ASIC holder while in a secure area. Should they become unsupervised for some reason, they must leave the secure area immediately.<sup>49</sup> To obtain a VIC, proof of identity is required, as is a declaration that the applicant has not been refused an ASIC, or had an ASIC cancelled or suspended due to criminal activity.<sup>50</sup>

5.55 An individual can be issued with a VIC in order to access a secure area across a particular security controlled airport for a maximum of 28 days within a 12 month period. This is known as the '28 Day Rule'.<sup>51</sup> However, there is a separate 28 day limit for each airport (the number of days a VIC has been issued at one airport does not count towards the number of days a VIC has been issued at a different airport). If the 28 days is reached, the person must apply for an ASIC or be denied access.<sup>52</sup>

5.56 The obligations of VIC issuers are set out in the Regulations. VIC issuers must ensure that VIC users are aware of their responsibilities, including returning the VIC card when finished with it, leaving a secure area if they are no longer supervised by an ASIC card holder, and complying with the 28 Day Rule.<sup>53</sup>

5.57 The committee understands that the VIC program underwent a number of changes in 2011. These changes were examined by the department in a Post

---

47 David Forsyth AM, Don Spruston and Roger Whitefield, *Aviation Safety Regulation Review*, May 2014, [https://infrastructure.gov.au/aviation/asrr/files/ASRR\\_Report\\_May\\_2014.pdf](https://infrastructure.gov.au/aviation/asrr/files/ASRR_Report_May_2014.pdf), p. 119; Australian Government, *The Aviation Safety Regulation Review Report – Government Response*, December 2014, p. 44.

48 Aviation Transport Security Regulations 2005, Part 6, Division 6.5, s. 6.38 and 6.38D.

49 Aviation Transport Security Regulations 2005, Part 3, Division 3.1, s. 3.09.

50 Department of Infrastructure and Regional Development, *Information for visitors to secure areas of airports*, December 2015, <https://infrastructure.gov.au/security/identity/aviation-security-information/visitor-secure-area-airport.aspx> (accessed 2 February 2017).

51 Aviation Transport Security Regulations 2005, Part 6, Division 6.5, s. 6.38E.

52 'Information for visitors to secure areas of airports', Department of Infrastructure and Regional Development, December 2015, <https://infrastructure.gov.au/security/identity/aviation-security-information/visitor-secure-area-airport.aspx> (accessed 2 February 2017).

53 Aviation Transport Security Regulations 2005, Part 6, Division 6.5, s. 6.40.

Implementation Review (PIR) in 2014, which identified a number of administrative areas where the VIC scheme could be improved.<sup>54</sup>

### ***Background checking***

5.58 While VIC holders do not require any background checking, since 1 November 2016 employees involved in issuing VICs must hold at least a white ASIC card, to prove they have undertaken a background check. Additionally, VIC holders must always be accompanied on airport grounds by a valid ASIC card holder.

5.59 The OTS has argued that:

Visitor supervision requirements largely mitigates many of the risks associated with allowing non-background checked individuals into secure areas....However, it became evident over time that in some cases VICs were being used to avoid background checking requirements. In response, the Department in cooperation with industry, undertook a policy development process to identify and implement policies to significantly strengthen visitor management, culminating in the enhancements to the Regulations.<sup>55</sup>

5.60 The committee acknowledged the changes requiring an ASIC holder to hold a valid background check to issue VICs. However, the fact that an ASIC card holder had a background check and can issue a VIC, does not change the fact that the VIC holder may not be suitable to enter an airport secure area.

5.61 The committee considered that there is no realistic way in which to police whether VIC holders are being accompanied by ASIC holders in real time, across all of Australia's airports. Unless actively monitored at each airport, this appears to be an area of high security risk.

5.62 An acknowledgement of this issue was made in the PIR, which stated, in relation to smaller and more remote airports:

Some airports face the difficulties of adhering to VIC requirements when the airport is manned by a limited number of staff. Various airports have indicated that the current regulations make it difficult, if not impossible, to supervise visitors and also conduct their operational duties relating to incoming aircraft.

---

54 'Visitor identification card (VIC) enhancements', Department of Infrastructure and Regional Development, [https://infrastructure.gov.au/security/files/Visitor\\_identification\\_card\\_VIC\\_enhancements.pdf](https://infrastructure.gov.au/security/files/Visitor_identification_card_VIC_enhancements.pdf) (accessed 23 January 2017).

55 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, p. 4.

---

...the requirement to supervise visitors away from a core area, has the potential to inadvertently decrease the security outcome at that airport.<sup>56</sup>

5.63 The PIR provided examples of where VICs were not issued at smaller, regional airports. Itinerant pilots arriving from non-security controlled airports, and not holding an ASIC, could refuel and leave without obtaining a VIC. Likewise, hobbyist pilots may bring guests to an airport without obtaining VICs and without regard to the security regulations. The PIR undertook to consider better options for visitor management at smaller and remote airports.<sup>57</sup>

### **28 Day Rule**

5.64 The 2011 changes limited the 28 Day Rule to a 12 month period, for any one airport. As noted in the PIR, this was to ensure that 'frequent or non-genuine visitors to secure areas of airports are background checked', and cannot avoid ASIC requirements.<sup>58</sup>

5.65 The PIR found no instances of anyone trying to, or succeeding in, obtaining a VIC for greater than the 28 day period. Industry stakeholders argued that 28 days was an appropriate time for a person to be engaged with an airport before having to apply for an ASIC. The PIR analysis also found that the introduction of the 28 Day Rule 'resulted in a reported reduction of non-background checked people working or accessing secure areas of airports'.<sup>59</sup>

5.66 The committee was concerned to hear that the 28 Day Rule could still be open to manipulation, either accidentally or intentionally. The PIR argued the greatest risk to breaches of the rule was from software data entry errors:

Such errors include incorrect names, spelling or use of different identification when applying, this potentially leads to a person being recorded in a VIC register as multiple individuals and the 28 day rule being inadvertently or even intentionally breached.<sup>60</sup>

5.67 The committee also noted that as the 28 Day Rule can apply at different airports, in theory a VIC applicant could indeed be a 'frequent' airport visitor. In this

---

56 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, p. 8.

57 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, pp. 8-9.

58 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, p. 4.

59 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, p. 10.

60 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, p. 12.

way, a VIC user with an adverse background could circumnavigate the requirement for an ASIC by exploiting the 28 Day Rule.

### ***VICs and contractors***

5.68 In relation to screening officers, the department confirmed to the committee that these officers were to hold and display a valid ASIC at all times. Screening officers in training, who had applied but were waiting for an ASIC, could use a VIC, provided they were 'not making independent screening decisions, and [were] constantly supervised by a qualified screening officer'.<sup>61</sup>

5.69 However, evidence received by United Voice indicated that in some cases subcontractors were being continuously issued with VICs in place of an ASIC, or using expired VICs. It argued that the use of VICs in place of ASICs could constitute a significant security risk, given that some companies appeared to rely on VICs for a significant proportion of their employees, and to avoid ASIC processing times.<sup>62</sup>

5.70 The PIR noted instances where a discretionary ASIC applicant was found to be working under a VIC, despite being refused an ASIC. The employer had no knowledge that the initial ASIC had been refused.<sup>63</sup>

5.71 Additionally, evidence to the PJCLE indicated that the high turnover of security guards meant that up to 25 per cent operated using the less-stringent VIC rather than a full background-checked ASIC.<sup>64</sup>

5.72 Amendments to the ASIC and VIC schemes since 2011 have gone some way to address these issues. Under questioning from the committee, the department noted that law enforcement, including police, AFP and Customs have authority to monitor VIC cards for compliance. The committee noted evidence it had received that expired VIC cards were in use, with the department responding:

The challenge is that, until we actually see that they are doing something wrong, we cannot act. We do not have officers at the airports all the time. So it is a matter of when we are there as to whether we are actually picking up those breaches that they may be committing.<sup>65</sup>

---

61 Correspondence from Ms Sachi Wimmer, Office of Transport Security responding to the committee's request for further information, received 15 February 2016, p. 3.

62 United Voice, *Submission 18*, pp. 10-11.

63 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, p. 13.

64 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, June 2011, p. 35.

65 Ms Sachi Wimmer, Office of Transport Security, Department of Infrastructure and Regional Development, *Committee Hansard*, 6 February 2015, p. 65.



5.73 The department noted it was the responsibility of industry stakeholders to ensure that the relevant screening officers and other employees used VICs appropriately, and complied with the regulations.<sup>66</sup> However, the department undertook a compliance program, consisting of annual audits, inspections and system testing.<sup>67</sup>

5.74 Despite the 2011 enhancements and the PIR, the committee was concerned by evidence regarding the alleged improper use of VICs by airport security workers. The committee remains particularly concerned that VIC holders do not require any background checking, and that this still makes the VIC scheme open to exploitation.

5.75 In addition, amendments to the VIC scheme were noted to have a disproportionate effect on regional and rural airports. The PIR found that despite efforts to 'tailor' arrangements for smaller airports, the VIC changes increased regulatory requirements at regional airports, and restricted 'the management operations of the airport due to staffing levels'. The PIR went on to state that:

maintaining the current arrangements at smaller/regional airports would continue to restrict their ability to apply more appropriate, tailored security measures which can have a similar security benefit but reduce the cost burden on industry.<sup>68</sup>

## **Committee view and recommendations**

### ***Shortcomings of the Aviation Security Identification Card***

5.76 The committee notes that the ASIC scheme has undergone constant review and alteration, particular in recent years and within the heightened security environment. While the committee is supportive of strong and effective security screening and processes, it acknowledges concerns regarding the impact of constant review and change to the ASIC regime.

5.77 Ongoing change makes it difficult for regulators, issuers, card holders and airports to understand and apply the most current version of the regulations and the most stringent security parameters. Constant change also leads to confusion and therefore increases the scope for people to circumnavigate the ever-changing rules.

5.78 It appears to the committee that the number of ASIC issuing bodies has decreased from 188 at the time of the Wheeler Review to 44 currently. However, the Wheeler Review noted these bodies were not linked or consistent, and, despite

---

66 Mr Steve Dreezer, Office of Transport Security, Department of Infrastructure and Regional Development, *Committee Hansard*, 6 February 2015, p. 65.

67 Ms Pauline Sullivan, Office of Transport Security, Department of Infrastructure and Regional Development, *Committee Hansard*, 6 February 2015, pp. 66-67.

68 Visitor Identification Card Enhancements Post Implementation Review, Maritime, Identity and Surface Security, Office of Transport Security, 2014, pp. 7-8.

recommendations for a single, centralised, government-run issuing body, there are still various issuing bodies.<sup>69</sup>

5.79 Given the importance of the ASIC, and the increased requirements for background checking proposed under the transport security bill, the committee urges the Australian Government to consider the feasibility of establishing a centralised issuing authority. Such an approach would likely lead to improved security outcomes.

### **Recommendation 5**

**5.80 The committee recommends that the Australian Government review the feasibility of establishing a centralised issuing authority for Aviation Security Identification Cards.**

#### *Self-reporting*

5.81 The committee upholds the view that the current self-reporting arrangement for ASIC holders convicted of an offence is not satisfactory, and raises significant security risks. This self-reporting system is not amended by the transport security bill, despite providing an opportunity to start addressing this issue.

5.82 Given this, the committee recommends that the Australian Government work with federal bodies and state stakeholders to investigate the possibility of a national integrated notification system for the sector. This would go some way to closing potential vulnerabilities in the current ASIC provisions.

### **Recommendation 6**

**5.83 The committee recommends that the Australian Government consider the development of a national automatic notification system for aviation-security-relevant offence convictions of Aviation Security Identification Cards holders.**

#### *Alleged misuse of Visitor Identification Cards*

5.84 The committee was concerned by evidence regarding alleged incidences of inappropriate VIC usage. The committee heard allegations that the current system may allow some misuse of VICs by unscrupulous security service providers, and by users who wish to avoid background checks.

5.85 The committee sees the lack of a background check for VIC holders as a considerable risk to aviation security. The committee appreciates that in some instances, a VIC may only be required for a very short period of time, and a

---

69 See for example Parliamentary Joint Committee on Law Enforcement, *Inquiry into the adequacy of aviation and maritime security measures to combat serious and organised crime*, June 2011, Recommendation 22, pp. 111-114.

background check is not realistic. This short timeframe does not, however, reduce the risk should someone be inclined to nefarious activity.

5.86 The fact there is a separate 28 day VIC limit for each airport, and no background check required for a card holder, appears to the committee to be an area of substantial risk. Additionally, the heightened level of offences under the ASIC/MSIC scheme to address serious and organised crime, proposed under the transport security bill, will not apply to someone casually entering secure airport areas under a VIC.

5.87 The committee is also concerned by evidence which revealed that the legal requirement to ensure that all VIC users are accompanied by an ASIC card holder at all times was not being adhered to. This presents a clear security risk, particularly in light of the fact that VIC holders are not background checked.

### **Recommendation 7**

**5.88 The committee recommends that the Department of Infrastructure and Regional Development update the committee early in 2018, on progress and outcomes, following implementation of Stage Two of the Visitor Identification Card enhancements.**

### **Recommendation 8**

**5.89 The committee recommends the Australian Government consider mechanisms, including legislative amendment, to strengthen the Visitor Identification Card process, incorporating appropriate background checking where appropriate.**

