

UNCLASSIFIED



Australian Government
Australian Security
Intelligence Organisation

**ASIO submission to the
Rural and Regional Affairs and Transport
References Committee inquiry
into Aviation and aviation security
January 2015**

Terms of Reference

On 4 December 2014, the Senate moved that the following matters be referred to the Rural and Regional Affairs and Transport References Committee for inquiry and report by 26 April 2015.

- a. recent media reports on apparent breaches in airport and aviation security at Australian airports;
- b. consideration of the responses to those reports from the Government, regulators, airports and other key stakeholders, and the adequacy of those responses;
- c. whether there are further measures that ought to be taken to enhance airport security and the safety of the travelling public;
- d. the findings of, and responses to, reports undertaken into airport security issues since 2000; and
- e. any related matters.

Submissions should be received by 16 January 2015. The reporting date is 26 April 2015.

Introduction

This submission is intended to provide the Committee with an overview of the role of the Australian Security Intelligence Organisation (ASIO) in contributing to the security of Australia's airports.

The submission includes a description of the role of the Organisation in providing national security threat assessments, and an overview of the current threat environment in Australia, and the terrorism threat to the aviation sector specifically. The information provided is unclassified, and therefore is mostly of a general nature.

The current threat environment: Aviation sector and airports

Terrorists retain an enduring intent to attack Western civilian aviation, as demonstrated in multiple attempts since 2001. Terrorist rhetoric and publications—most recently the thirteenth edition of AQAP's *Inspire* magazine—reinforce terrorists understanding of the widespread economic and social damage a successful attack against civilian aviation targets can inflict. We expect civilian aviation will remain a high-value terrorist target for the foreseeable future.

The repeated attempts by terrorist groups since 11 September 2001 to attack Western civilian aviation targets have demonstrated the capability to employ sophisticated improvised explosive devices (IEDs) using innovative and effective concealment techniques. The progression of attack methodologies demonstrates adaptation to security measures and refinement of previous attack methods.

- In May 2012, United States (US) officials announced they had seized an IED similar to the underwear-concealed device used in the 2009 attack against Northwest Airlines 253.
- On 29 October 2010, an intelligence tip-off led to the discovery of two IEDs concealed within two separate air cargo consignments bound for the US. AQAP claimed responsibility for the attack.
- On 25 December 2009, AQAP operative Umar Farouk Abdulmutallab attempted to detonate an IED concealed in his underwear aboard a Northwest Airlines flight from Amsterdam to Detroit. The

explosives failed to detonate correctly, causing a fire. Abdulmutallab was subdued by passengers and flight crew and was arrested on arrival in Detroit.

- In 2006, a plot to detonate liquid explosives on-board at least 10 airliners travelling from the United Kingdom to the US and Canada was disrupted.
- On 22 December 2001, al-Qa'ida affiliate Richard Reid attempted to detonate explosives concealed in shoes aboard an American Airlines flight travelling from Paris to Miami. Passengers noticed Reid's attempts to light a fuse in his shoes and subdued him. A second operative, Saajid Badat, also received a shoe-concealed IED, but did not catch his flight and was subsequently arrested.

Airports are also attractive targets for terrorists, as demonstrated by attacks overseas. The open and accessible nature of some airport areas and the concentration of large crowds make airports more susceptible to low-capability attack.

- In September 2014, three individuals were arrested after parking a vehicle containing IEDs in the car park of Manila's Ninoy Aquino International Airport.
- In November 2013, Paul Ciancia shot dead a Transportation Security Administration official at Los Angeles International Airport. Ciancia continued firing as he moved through the terminal building, wounding three more people, before being shot by police and arrested.
- In July 2012, an IED detonated onboard a bus transporting Israeli tourists at the Burgas Airport in Bulgaria, killing seven and injuring 32.
- In March 2011, a gunman attacked US Air Force personnel outside a terminal building at Frankfurt Airport in Germany, killing two and injuring two more.
- In January 2011, a suicide bomber detonated an IED in the international arrivals hall of Domodedovo Airport, Moscow. The explosion killed 37 and injured more than 160.
- In June 2007, a vehicle loaded with propane canisters was driven into the front entrance of Glasgow International Airport and ignited. The vehicle did not enter the terminal, and damage was limited—the only fatality in the attack was one of the terrorists.
- In July 2002, an Egyptian national opened fire on passengers and staff at the El Al airline ticket counter at Los Angeles International Airport. The attacker killed two others before being killed by a security officer.

While not terrorism related, the March 2009 brawl at Sydney Airport Terminal Three between rival outlaw motorcycle gangs (OMCG) in which one OMCG member was killed, shows that Australia's airports are not immune from security incidents in front-of-house areas where access is relatively open.

Trusted Insiders – ASIO's role in ASIC checking

Terrorists have exploited the trusted access of individuals within the aviation sector in order to overcome security measures.

- In December 2013, US authorities arrested US citizen Terry Loewen as he attempted to gain access to Wichita Mid-Continent Airport runway areas. Loewen allegedly intended to attack aircraft on the tarmac using a vehicle he believed contained explosives. Loewen worked as an avionics engineer and had access and escort privileges to airport runways and infrastructure. However, Loewen's 'VBIED' did

not contain explosives and preparation was assisted by an undercover Federal Bureau of Investigations agent who Loewen believed was an AQAP operative.

- In February 2011, former British Airways information technology (IT) employee Rajib Karim was found guilty on four counts of preparing acts of terrorism, including using his access to British Airways computer systems to provide confidential information to AQAP-linked terrorists. Karim allegedly discussed with then senior (but now deceased) AQAP ideologue Anwar al-Aulaqi the potential to disrupt British Airways IT systems, using his position to get himself and others employment opportunities as cabin crew, and the potential to bring down a US-bound flight with explosives.

The Aviation Security Identification Card (ASIC) scheme was established by the Aviation Transport Security Act 2004 (ATS Act), the Aviation Transport Security Regulations 2005 (ATS Regulations). This regulatory framework seeks to safeguard aviation transport facilities against unlawful interference. Central to achieving this objective is the obligation for industry participants to develop and comply with security plans. The AusCheck Act 2007 and the AusCheck Regulations 2007 established the regulatory framework for coordinating and conducting certain criminal, security and other background checks. ASIO involvement in the ASIC process began in 2005. ASIO undertakes national security relevant checks for AusCheck on a cost recovery basis and conducted 75,015 ASIC checks in 2014.

Threat reporting

The National Threat Assessment Centre (NTAC) within ASIO provides assessments and advice on security threats to Australian interests at home and abroad, threats to Australian and overseas dignitaries, violent protest threats, threats to diplomatic premises in Australia, threats to critical infrastructure sectors, and threats to major events. The NTAC is Australia's national authority for threat assessments relevant to security as defined by the ASIO Act 1979. The NTAC integrates officers from a number of Australian counterpart agencies, enabling a fusion of sector knowledge that is vital to its effectiveness.

The NTAC produces threat assessments for all critical infrastructure sectors, including the Australian aviation sector, and in response to specific threat reporting or major security incidents overseas. Threat advice helps stakeholders – including airport operators – understand the environment so that they can plan and implement protective security arrangements and risk management strategies. The NTAC also produces a classified biannual analytical report focusing on the terrorist threat to the transport sector in Australia. These products include assessment of aviation-relevant threat reporting, which may include attacks on aviation infrastructure overseas.

The heightened threat environment saw Australia's public alert level raised from MEDIUM to HIGH—the first time this has ever occurred. The NTAC reviewed the terrorist threat to all critical infrastructure sectors, including aviation, in September 2014, when the general terrorism threat level was increased. The Australian aviation sector is broad and diverse; the level of threat to different operations may differ substantially. Accordingly, ASIO assesses the threat to discrete aspects of the sector. The terrorist threat to the Australian aviation sector remains under constant review.

Protective Security Advice Engagement

ASIO's protective security advice unit, T4, provides physical security advice to the Australian Government, state and territory governments, critical infrastructure sectors, and Australian businesses.

As a result of the Wheeler review into aviation sector security, The Department of Infrastructure, Office of Transport Security (OTS), engaged the services of T4 to undertake vulnerability analysis of all major Australian airports, and a selection of regional screened airports during 2008/09. The vulnerability assessments highlighted some deficiencies of existing security measures in mitigating terrorist attack methods. Acceptance and implementation of any recommended security improvements remains outside the authority of ASIO. ASIO T4 undertakes post-rectification reviews only at the request of the client.

Should OTS request updated vulnerability assessments, ASIO will seek to include that activity in our forward work program subject to any other higher national security priorities.

T4 provides a range of protective security advice to the aviation sector at their request—including protective security risk reviews and vulnerability assessments. These services are provided on a cost recovery basis.

Stakeholder Engagement

Operators of Australian airports are a major stakeholder. ASIO works closely with the Office of Transport Security and the Attorney-General's Department to convey threat information to airport operators in a timely manner. ASIO also regularly provides threat environment briefings to airport management committee meetings, including Airport Security Committee meetings at major airports, industry-wide Aviation Security Advisory Forums, and Regional Industry Consultative Meetings.

ASIO's Business Liaison Unit (BLU) provides intelligence-backed unclassified reporting to the aviation sector via the BLU secure website. The BLU also engages one-on-one with representatives from the major Australian airports; and Qantas and Virgin Australia.

The BLU hosts annual Aviation Sector classified briefing days. In 2014 this briefing was held in ASIO headquarters in conjunction with the Office of Transport Security. Classified briefings provide an opportunity for industry participants to receive detailed information and background on the range of security threats facing the aviation industry.

In February 2015, the BLU will commence a regional airports engagement program, to ensure security managers at Australia's regional airports are aware of the BLU website, utilise the range of information available to them and establish a personal point of contact for on-going engagement.