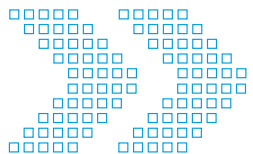




**Australian Government**  
**Australian Security  
Intelligence Organisation**

# ASIO Report to Parliament 2012–2013



[www.asio.gov.au](http://www.asio.gov.au)

# Our vision

The intelligence edge for a secure Australia.

# Our mission

To identify and investigate threats to security and provide advice to protect Australia, its people and its interests.

# Our values

## ACCOUNTABILITY

We are responsible for what we do and for our outcomes.

We are accountable to the Australian community through the government and the parliament.

## COOPERATION

We build a common sense of purpose and mutual support.

We communicate appropriately in all our relationships.

We foster and maintain productive partnerships.

## EXCELLENCE

We produce high quality, relevant, timely advice.

We display strong leadership and professionalism.

We improve through innovation and learning.

## INTEGRITY

We are ethical and work without bias.

We maintain confidentiality and the security of our work.

We respect others and value diversity.

The ASIO logo is a central graphic element consisting of a dark blue, three-dimensional cube with the letters 'ASIO' in a light, sans-serif font on its front face. The cube is surrounded by several overlapping, semi-transparent, light grey geometric shapes that resemble facets of a larger, more complex crystal or star-like structure, creating a sense of depth and modernity.

# ASIO Report to Parliament 2012–2013



ISSN 0815-4562

© Commonwealth of Australia  
(Australian Security Intelligence  
Organisation) 2013.



All material presented in this publication is provided under a Creative Commons (CC) BY Attribution 3.0 Australia Licence (<http://creativecommons.org/licenses/by/3.0/au/deed.en>).

The details of the relevant licence conditions are available on the Creative Commons website (<http://creativecommons.org/licenses/>) as is the full legal code for the CC BY Attribution 3.0 Australia Licence (<http://creativecommons.org/licenses/by/3.0/legalcode>).

## Commonwealth Coat of Arms

The Commonwealth Coat of Arms is used in accordance with *Commonwealth Coat of Arms: information and guidelines*, November 2012, provided by the Department of the Prime Minister and Cabinet ([http://www.dpmc.gov.au/guidelines/docs/CCoA\\_guidelines.pdf](http://www.dpmc.gov.au/guidelines/docs/CCoA_guidelines.pdf), viewed 9 May 2013).



**Australian Government**  
**Australian Security**  
**Intelligence Organisation**

Director-General of Security

31 October 2013

A7693101

Senator the Hon George Brandis QC  
Attorney-General  
Parliament House  
CANBERRA ACT 2600

*Dear Attorney,*

In accordance with section 94 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), I am pleased to present to you ASIO's Annual Report for the year ending 30 June 2013.

As required by the ASIO Act, a copy of the Annual Report – with deletions authorised by you to protect national security – is to be laid before each House of the Parliament.

In addition, as required by the *Commonwealth Fraud Control Guidelines*, I certify that I am satisfied ASIO has in place appropriate fraud control mechanisms that meet the Organisation's need and comply with the Guidelines.

*Yours,*  
*David Irvine*  
David Irvine

GPO Box 2175  
Canberra City ACT 2601  
Telephone: 02 6249 6239  
Facsimile: 02 6257 4501

**FOI WARNING:**  
Exempt document under  
Freedom of Information Act 1982.  
Refer related FOI requests to  
Attorney-General's Department, Canberra.



# Table of Contents

---

Director-General's foreword	vii
The year at a glance	x
Guide to the report	xi
ASIO's role and functions	xii
Organisational structure	xii

## Part 1

<b>The security environment 2012–13 and outlook .....</b>	<b>1</b>
Terrorism	2
Espionage	5
Foreign interference	6
Communal violence and violent protest	7
Border integrity	8

## Part 2

<b>Program performance.....</b>	<b>9</b>
Security intelligence analysis and advice	11
Protective security advice	22
Security intelligence investigations and capabilities	25
Foreign intelligence collection in Australia	29

## Part 3

<b>Outcomes and highlights .....</b>	<b>31</b>
--------------------------------------	-----------

## Part 4

<b>ASIO and accountability.....</b>	<b>35</b>
Attorney-General	36
Parliamentary oversight	36
Inspector-General of Intelligence and Security	38
Independent Reviewer of Adverse Security Assessments	39
Independent National Security Legislation Monitor	40
Legal assurance and capability protection	41
Other reviews	42
Internal audits and fraud control	43
Security in ASIO	45
Outreach	46

## **Part 5**

<b>Corporate management</b> .....	<b>49</b>
Corporate strategy and governance	50
People	54
Property	63
Financial services	65
Information and technology services	66

## **Part 6**

<b>Financial statements</b> .....	<b>69</b>
-----------------------------------	-----------

## **Part 7**

<b>Appendices and indices</b> .....	<b>115</b>
<b>Appendix A</b>	
Agency Resource Statement	116
<b>Appendix B</b>	
Expenses by Outcomes	117
<b>Appendix C</b>	
Mandatory reporting requirements for Questioning and Questioning and Detention Warrants under section 94 of the ASIO Act	118
<b>Appendix D</b>	
Workforce Statistics	119
<b>Appendix E</b>	
ASIO Salary Classification Structure at 30 June 2013	121
Compliance Index	123
Additional ASIO reporting requirements (under the ASIO Act)	128
Glossary	129
Index	131





## Director-General's foreword

---

ASIO's mission is to identify and investigate threats to security and provide advice to protect Australia, its people and its interests in Australia and overseas.

### Security environment in 2012–13

Influences in Australia's security environment have remained similar to those of previous years. Terrorism remains the most immediate threat to the security of Australians and Australian interests—yet other security threats have gained momentum.

The threat of home-grown terrorism is of significant concern—terrorist attacks such as the Boston Marathon bombings in the United States and the Woolwich attack in the United Kingdom demonstrate this. Home-grown terrorism and lone actors present unique and difficult challenges for security agencies.

Terrorist organisations, such as al-Qa'ida and its affiliates, remain committed to conducting and promoting mass casualty attacks. They continue to encourage vulnerable individuals to commit attacks on ordinary citizens. The threat of terrorist attacks on Australians and Australian interests abroad remains of concern. ASIO works with domestic and international partners to identify, investigate and mitigate such threats.

There has been an increase in Australians travelling overseas to participate in terrorist training or engage in foreign disputes—Syria is the primary destination. The concern is not only for Australians who risk their lives overseas, but also the likelihood of radicalised Australians returning home with an increased commitment and capability to pursue violent acts on our shores.

The Syrian conflict has also created domestic tensions. Communal violence within our borders does occur, and, while all cultures have a place in Australian society, violence should not.

In response to these many threats, ASIO has contributed to the defence of Australia's interests through the disruption of terrorist planning in Australia, the prevention of Australians seeking to travel overseas to participate in violent extremist activity and the identification and prevention of violent extremism within the Australian community. These actions were conducted in partnership with law enforcement, national and international partners.

Instances of espionage and foreign interference have continued to increase—both in terms of the number of occurrences and the range of actors.

The ability to prevent foreign countries conducting espionage or sabotage by cyber means is an important element in our national wellbeing. ASIO will continue to cooperate with partners, as well as industry and owners of national infrastructure, to offset the hostile and pervasive nature of this threat.

Espionage activity extends to the threat of a 'trusted insider'. International high-profile cases this year serve as a reminder of the risk that someone with legitimate access to classified systems may deliberately disclose or sell protected information. Though not of the same scope or scale, there have been a number of cases in Australia of unauthorised removal, dissemination or mishandling of sensitive material by trusted employees. Internal security measures are paramount in preventing and combating such disclosures.

## Legislative reform

Developments in the telecommunications sector are rapid. Proposed reforms to the *Australian Security Intelligence Organisation Act 1979*, the *Intelligence Services Act 2001*, the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979* are critical to ensuring the effective conduct of ASIO's work, while also ensuring high levels of accountability.

The findings of the Parliamentary Joint Committee on Intelligence and Security inquiry into these proposed legislative reforms remain under consideration by the government.

## Budgetary outlook

The government will continue to operate in a tight fiscal environment for the foreseeable future, which will naturally have flow-on effects on ASIO. This has placed further importance on the ability of ASIO to ensure resources are placed against the highest security risks, without any diminution in Australia's national security capability.

## Public engagement

This year I have continued my concerted effort to provide greater visibility of ASIO's work. While there will always be limitations on the public disclosure of operational matters, I have taken the opportunity from time to time to discuss the nature of ASIO's business with the general public, community groups and forums. Public speeches I have given have been made available on the ASIO website.

ASIO has also appeared at Senate Estimates and parliamentary hearings, released publications and published general information on the ASIO website.

As a security intelligence organisation, ASIO's contact with the media is limited as ASIO does not comment on individual cases or investigations. Nevertheless ASIO will continue to engage with the media as often as appropriate.

I trust this report will provide some insight into the work of the nameless people of ASIO, who are to be commended for their conscientious professionalism in the support of national security and the safety and lives of their fellow Australians.

**David Irvine**

Director-General of Security

# The year at a glance

## ASIO'S WORK

ASIO identified, investigated, and analysed threats to security posed by terrorism, espionage, foreign interference, the promotion of communal violence, sabotage, threats to Australia's defence and people smuggling.

Of particular note, ASIO:

- ▶ investigated several hundred mostly Australia-based individuals who are advocates of a violent Islamist ideology;
- ▶ managed the security threat posed by individuals working with al-Qa'ida affiliated groups, including in Syria;
- ▶ worked closely with partner agencies to identify and mitigate the threat to the security of government information from the 'trusted insider';
- ▶ degraded the harmful activities of foreign intelligence officers working in Australia against Australian interests;

- ▶ provided Australian government agencies with intelligence on people smugglers and their ventures to support surveillance, interdiction and disruption activities; and
- ▶ developed a new cyber defence and cyber protection capability to counter the espionage and sabotage capabilities that are now possible through cyber means.

ASIO completed:

- ▶ 130 045 counter-terrorism security assessments;
- ▶ 29 449 visa security assessments (an increase of 5352 over the 2011–12 figure); and
- ▶ 27 586 personnel security assessments.

## CORPORATE STRATEGY AND GOVERNANCE

During the reporting period, ASIO:

- ▶ developed a new *ASIO Strategic Plan 2013–16*, which builds on the solid foundation of the previous plan and will ensure ASIO is prepared for the complex security environment we face now and into the future. It will allow ASIO to focus on its critical priorities while responding with agility and resilience to emerging challenges. Further details can be found on pages 50 and 51;
- ▶ developed a technical capabilities workforce plan to address the unique challenges of attracting and retaining quality technical and information technology staff in a security environment; and
- ▶ developed the Management and Leadership in Security Intelligence strategy to build management and leadership capability and expertise.

# Guide to the report

---

In accordance with section 94(1) of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), the Director-General of Security provides a report to the Attorney-General on the activities of ASIO for the year ending 30 June. The Attorney-General is required to table an unclassified version of this report, in each House of the Commonwealth Parliament, within 20 sitting days of receipt.

The annual report is an opportunity for ASIO to communicate information regarding its work to parliament, government, stakeholders and the public. It is a key component of ASIO's accountability framework.

**Part 1** summarises the security environment in which ASIO has operated.

**Part 2** reports on ASIO's performance in providing relevant advice and information to government and other stakeholders.

**Part 3** is a detailed report of ASIO's performance and operations against the key outcome of protecting Australia and its people from threats to security. This section is classified Top Secret and is excluded in its entirety from the unclassified version of the report for reasons of national security.

**Part 4** outlines ASIO's oversight and accountability mechanisms and provides information on a range of audits and reviews, both internal and external, to which ASIO has contributed.

**Part 5** provides information regarding the management and corporate services functions of ASIO.

**Part 6** details ASIO's financial statements for the 2012–13 financial year.

**Part 7** provides additional information regarding ASIO's finances and resources, as required by legislation.

# ASIO's role and functions

---

ASIO is responsible for the protection of Australia, its people and its interests from threats to security, whether directed from, or committed within, Australia or overseas.

ASIO does this by collecting, analysing and evaluating intelligence relevant to security and providing advice to ministers, Commonwealth and state authorities, and other entities approved by the Attorney-General.

The ASIO Act defines 'security' as the protection of Australia and its citizens from:

- ▶ espionage;
- ▶ sabotage;
- ▶ politically motivated violence;
- ▶ the promotion of communal violence;
- ▶ attacks on Australia's defence systems;
- ▶ acts of foreign interference; and
- ▶ serious threats to Australia's territorial and border integrity.

The ASIO Act also authorises ASIO to:

- ▶ provide security assessments, including for entry to Australia, access to classified material and access to designated security-controlled areas;
- ▶ provide protective security advice;

- ▶ obtain foreign intelligence within Australia, under warrant, at the request of the Minister for Defence or the Minister for Foreign Affairs;
- ▶ communicate and cooperate with Commonwealth agencies and departments, police forces, and authorities of the states and territories; and
- ▶ communicate and cooperate with relevant authorities of foreign countries, as approved by the Attorney-General.

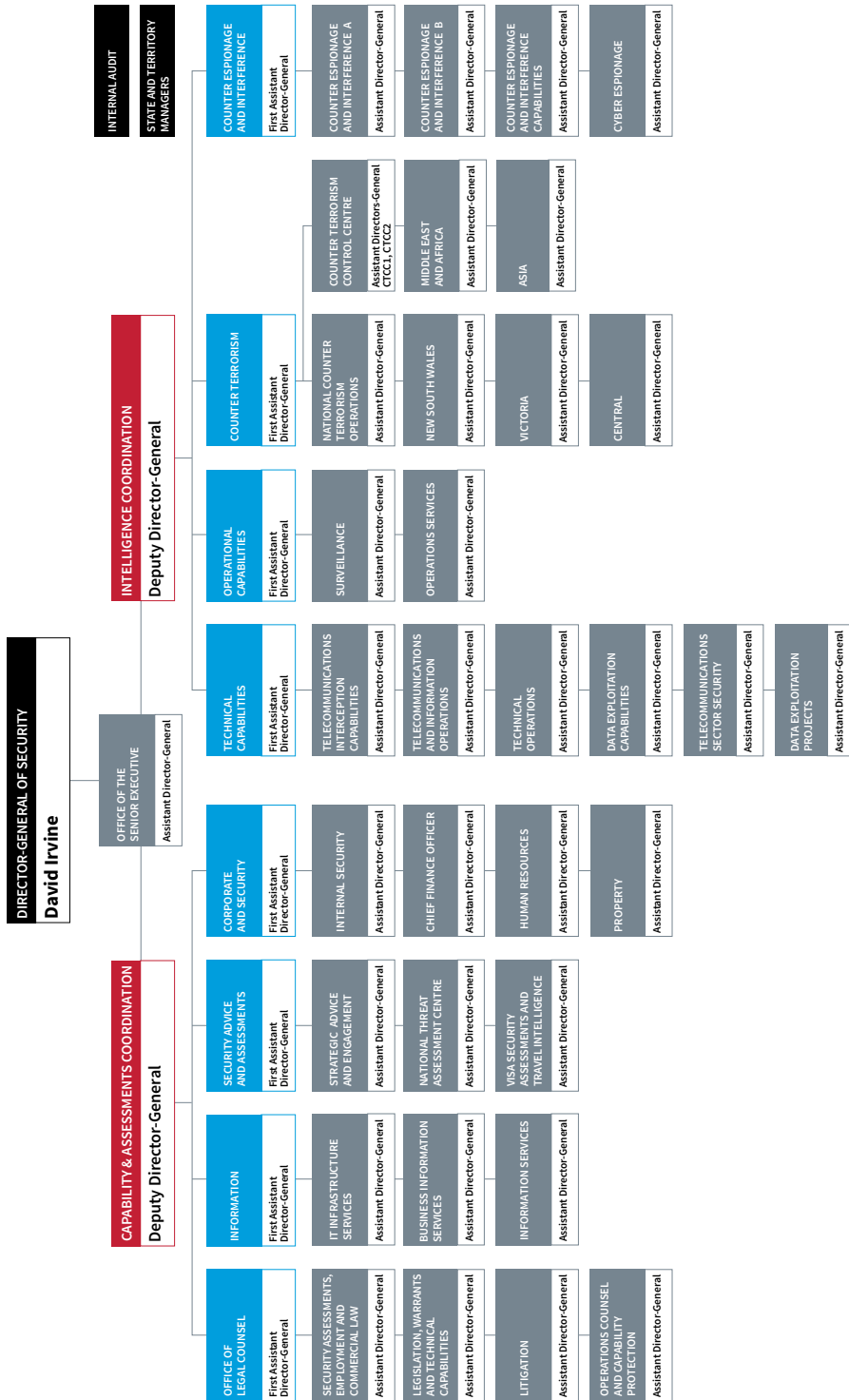
In the performance of functions such as investigating and responding to threats, ASIO works closely with a range of stakeholders, including state and federal law enforcement agencies, members of the Australian Intelligence Community, government departments, industry and international liaison partners.

## Organisational structure

---

As forecast in the previous year, ASIO continued to consolidate and refine its organisational structure in 2012–13 after a period of substantial growth. On 17 January 2013 ASIO adopted a new organisational structure, which reduced the number of divisions from 11 to eight. ASIO reduced the size of its Senior Executive Service by 25 per cent through a voluntary redundancy program.

# ASIO's organisational structure as at 30 June 2013









# Part 1

## THE SECURITY ENVIRONMENT 2012–13 AND OUTLOOK

‘It is ASIO’s assessment that Australia remains a target for a range of individuals and groups who would promote their belief systems and seek to destroy our democratic way of life—not by some imagined, slow-time conspiracy or slow-burning action, but in a violent and irreversible instant.’

► *Speech by the Director-General to the Security in Government Conference  
4 September 2012*

Australia, its people and its interests can be harmed by a range of activities undertaken by domestic or foreign actors. ASIO's role is focused on detecting, investigating and advising on acts of espionage, sabotage, politically motivated violence—including terrorism—the promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and serious threats to Australia's territorial and border integrity. ASIO aims to anticipate or detect the actions of those who would harm us and to provide advice to prevent harm from occurring, through either intervention and the disruption of activities or the implementation of security measures to protect against harmful actions.

For the most part, the activities that might harm us are strongly influenced by a range of evolving factors which mostly occur, or originate, overseas. The threat from terrorism is strongly linked to political, ideological and cultural conflicts elsewhere. In particular, the complex interconnected issues around the Syrian conflict, tensions across the Middle East, and the aftermath of the Arab Spring will continue to present a variety of security challenges to Australia in the foreseeable future.

Espionage, foreign interference and malicious cyber activity undertaken by foreign powers can have a serious negative impact on Australia's national interests. The unauthorised disclosure of official and classified information by individuals or groups remains an area of concern, requiring constant vigilance.

## Terrorism

---

The threat to Australia from terrorism remains real, ongoing and evolving.

The terrorism threat posed by traditional extremist networks and groups is being compounded by self-radicalising lone actors motivated both by an extremist ideology which advocates 'stand-alone, stay at home' attacks and participation in violent extremism overseas.

In Australia, there are individuals and small groups who believe an attack here is justified. Issues such as Australia's military deployments over the last decade, the Syrian conflict, or a belief that the ideals of Australia are in direct conflict with their extreme interpretation of Islam, fuel the radical views of this cohort.

Recent overseas attacks have utilised basic capabilities and simple technologies, demonstrating that an attack need not be complex to achieve the goals of the perpetrators.

In April 2013 two bombs were detonated at the Boston Marathon, killing three people and wounding over 200. One month later, a British soldier was murdered in public in the United Kingdom. These unrelated attacks were perpetrated, without apparent external coordination or direction, by disenfranchised and radicalised individuals utilising everyday items which required no unique skill or knowledge that could not be gained from simple online instructions. The threat of lone actors presents a significant challenge for security and law enforcement agencies—notably the difficulty of identifying such individuals quickly enough to disrupt an attack.

*Inspire 10*, the English-language magazine of al-Qa'ida in the Arabian Peninsula



These attacks demonstrate the key terrorist priorities of engendering community anxiety, supporting the broader Islamist extremist strategy of ‘death by a thousand cuts’ and adhering to the ‘think globally, act locally’ message that features in radical rhetoric.

This evolution in terrorist modus operandi does not supplant the ongoing threat posed by more organised and directed extremist groups, which continue to aspire to conduct large-scale, mass-casualty attacks against the West.

Australia is not immune to radicalisation processes. Information and communications technologies have helped spread the extremist message, and this trend continues. In particular, social networking platforms have expanded the ways by which extremists communicate and share their ideologies and methods. Extremist material such as *Inspire*, the English-language magazine of al-Qa'ida in the Arabian Peninsula (AQAP), continues to provide instruction, and encourage individuals to conduct unilateral attacks, often with no direct contact or coordination from senior extremist leaders. References to Australia in publicly available extremist material confirm groups such as al-Qa'ida continue to regard Australia as a legitimate target of terrorist attacks.

Ongoing conflicts overseas present a range of security challenges for Australia.

The Syrian conflict has resonated strongly in Australia, partly because of deep familial ties to Lebanon that exist here. Many Australians—a significantly greater number than we have seen for any comparable conflict—have travelled to the region, including several to participate directly in combat or to provide support to those involved. As at 30 June 2013, four Australians were known to have been killed in Syria.

ASIO is concerned about the potential for Australians in Syria to be exposed further to extremist groups and their ideology. Such groups include the recently proscribed terrorist organisation Jabhat al-Nusra. An individual who becomes involved in the conflict and who holds, or develops, an extremist ideology could return to Australia not only with the intent to facilitate attacks onshore but also with experience and skills in facilitating attacks. In addition, the individual's social connections with international fighters could make such attacks easier to carry out. Alternatively, such an individual could become involved in terrorist activity elsewhere, exploiting the relative travel advantages Australian citizenship brings.

We expect these challenges to play out over several years and have a medium- to long-term influence on the extremist environment in Australia, beyond any immediate resolution to the Syrian civil war.

Another by-product of the Syrian conflict has been sporadic incidents of small-scale communal violence in Australia along the lines of the Middle East's Sunni-Shi'a divide. Strong leadership by the Islamic community leaders has so far helped largely contain communal tension of this sort in Australia.

Afghanistan, Pakistan and Yemen continue to appeal as destinations for those pursuing an extremist ideology. Security challenges persist in Somalia. Areas of North Africa that have seen political changes resulting from the Arab Spring have emerged as new arenas for terrorist training, facilitation and attack planning. The 16 January 2013 attack against the In-Amenas oil facility in southern Algeria by an al-Qa'ida-linked group demonstrates that extremists have the intent and capability to attack critical commercial infrastructure in the region.

Kidnap-for-ransom operations targeting Westerners also continue to be a favoured modus operandi of extremists in Africa, the Middle East and South Asia. Despite intense counter-terrorism pressure, AQAP remains resilient, innovative and ambitious; it poses a significant threat within Yemen and represents the most likely al-Qa'ida affiliate to conduct a transnational attack.

The terrorism threat in Indonesia is enduring. Despite the admirable successes of counter-terrorism operations throughout South-East Asia, a range of extremist groups in the region continue to have an interest in preparing and conducting attacks against Western interests locally, including against Australians.

Australian interests in Indonesia continue to be regarded as a legitimate target. The impending release of terrorist detainees from Indonesian prisons, a spike of which is expected to occur in 2014, is likely to increase this threat. Many of the individuals scheduled to be released in this period have undertaken terrorist training or have been linked to, or involved in, bombings against either Western or local targets. Their release is likely to inject significant capability into extremist networks. The expertise and anti-Western credentials of some individuals have the potential to refocus and reinvigorate currently diffuse and relatively unsophisticated extremist networks.

# Espionage

---

Espionage targeting Australian interests remains a serious and sustained threat to Australia's national security. Any Australian government information which is not publicly available will continue to be actively sought and leveraged by some foreign governments, which will allocate clandestine intelligence collection resources for this purpose. In the modern world, the threat and potential harm to Australia's interests from such activity is broader than national security, defence or sensitive foreign policy. With the competitive global economy and the prominence of Australia in a number of key market sectors, economic information, science and technology data and intellectual property are increasingly highly valued and priority targets of foreign espionage activities conducted against Australia.

Many foreign governments have a broad range of intelligence capabilities that can be called upon as required. These include both human and technical capabilities that can be deployed in a variety of scenarios.

In recent years the Australian Intelligence Community has seen the scale and sophistication of cyber espionage conducted against Australian government and private sector systems increase significantly. Malicious cyber activity can be the most visible manifestation of foreign espionage activities against Australia and highlights the interest and value to foreign entities in accessing and using protected or sensitive Australian information. Working collaboratively with its key national security partners, ASIO and the Computer Emergency Response Team (CERT) Australia are heightening awareness with the public and private sectors of the very real threat posed by espionage facilitated through the internet, and to harden defensive responses – both at the technical and human level.



The betrayals of trust by individuals who have gained legitimate access to national systems and environments is a constant source of potential harm to Australia's national interests. Whatever the motivations or allegiances of such individuals, such cases demonstrate the considerable vulnerability arising from the aggregated storage of sensitive information on systems which can be exploited by individuals with authorised access to those systems.

Successful clandestine foreign intelligence service penetration of the Australian government has the potential to cause significant damage to Australian national interests. These matters bring into sharp focus the need to maintain robust and rigorous standards when assessing an individual's suitability for access to classified material.

ASIO places high priority on raising awareness among government agencies and industry of espionage threats facing Australia. ASIO works closely with partners across government and industry to provide security intelligence advice and to heighten awareness of the threat environment. ASIO's engagement and input are central in driving and shaping appropriate security policy responses.

The threat and harm posed by espionage activities are multifaceted and ASIO's defensive response must reflect this. Partnerships between government and industry are pivotal in ASIO's mission to discover, defend against, and degrade these activities, and to provide a holistic protective security response.

## Foreign interference

---

Foreign interference has the potential to cause significant harm to Australia's national sovereignty and independence of government and can undermine the security and safety of our citizens and residents. Foreign interference can also manifest in the intention and desire to covertly subvert and influence Australia's political processes and outcomes to meet foreign government objectives. Foreign interference threatens the safety and well being of members of the Australian community and may involve coercion, threats or even physical harm to the individual or to their family members.

Within Australia's democratic, pluralistic society, members of the community have the right to engage in peaceful dissent, whether directed towards Australian political processes or the political processes of a foreign government.

ASIO works vigorously to detect and defend against foreign interference activities to ensure individuals in Australia are not harassed, intimidated or harmed by foreign governments or their representatives. Often the most vulnerable members of a community are targeted. Through threats and coercion, they are forced to report on other community members or pressured to illicitly obtain information to assist a foreign government to monitor individuals and communities in Australia. Incidents of foreign interference were detected and investigated by ASIO across a broad cross-section of communities.

Foreign powers will continue to seek to interfere clandestinely and deceptively in Australia's domestic affairs and against Australia's interests, including in the political, commercial and business sectors, and through monitoring expatriate communities. In response, ASIO has increased its investigative capability and resourcing to address the threat of foreign interference to Australian interests.

## Communal violence and violent protest

---

Section 17A of the ASIO Act expressly prohibits ASIO from investigating peaceful and lawfully conducted protest or advocacy activity. ASIO investigates protest activity only when it includes, or has the potential to include, planned violent activity or where it has the potential to impinge on the security of certain designated persons and places. However, ASIO may prepare threat assessments in relation to demonstration or protest activity on the basis of information it already has or which is passed to it by other agencies. ASIO's threat assessment function is an integral part of national arrangements for the protection of high office holders, internationally protected persons, sites of national significance and critical infrastructure.

ASIO remains vigilant in regard to those who may seek to use protests as a vehicle for inciting violence by deliberately using tactics likely to provoke a violent reaction. During 2012–13 we saw elements of this approach in Australia, as well as related heightened tensions between anti-Islam groups and Islamist extremists.

The Syrian conflict has exacerbated pre-existing political and sectarian divisions in Australia, which has led to a range of threats and acts of communal violence during the past year by both pro- and anti-Syrian Government supporters.

On 15 September 2012 a protest in Sydney against the film *Innocence of Muslims* turned violent when several members of a wider protest group clashed with police. The clashes represented one of the most public examples in Australia of individuals willing to use violence in what they perceived as the defence of Islam. Condemnation from local Islamic community leaders, the subsequent police response and the widespread public outcry combined to prevent further violent protest activity or retaliatory action.

ASIO anticipates the Group of Twenty (G20) meetings in 2014 may attract protest activity. The G20 summit brings together international leaders; it represents the world's largest economies and it attracts global media coverage. Most protests are expected to be peaceful; however, destructive, disruptive and confrontational protest tactics have been used at previous G20 meetings. Additionally, extreme groups such as anarchists could seek to participate in, and use the cover of, mainstream protests to undertake and incite violence.

## Border integrity

---

ASIO continues to contribute to the whole-of-government effort to counter serious threats to Australia's border and territorial integrity. Over the past 12 months, ASIO's contribution has included identifying and investigating Australians and Australia-based individuals involved in maritime people smuggling, and providing appropriate advice to government.

People smugglers continue to exploit established unauthorised maritime 'pipelines', and there has been an increase in unauthorised maritime arrivals over the 2012–13 reporting period.

The majority of individuals arriving in Australia pose no security threat. However, the activities, connections, capability and ideology of some individuals arriving in Australia require investigation by ASIO to determine whether they pose a risk to Australia's security.





# Part 2

## PROGRAM PERFORMANCE

‘We make predictive judgements about what may happen, and if we get it wrong it can have a catastrophic impact on the safety of the community. It places great stress within ASIO to decide whether the community or the individual should get the benefit of doubt in an assessment.’

► *Speech by the Director-General to the Biennial Conference of the District and County Court Judges [of Australia and New Zealand]  
26 June 2013*

ASIO's outcome statement was revised in the 2012–13 Portfolio Budget Statements to reflect better the Organisation's mandate to the Australian Government.

## OUTCOME 1

To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government.

ASIO's outcome supports the Australian government's policy aim of 'A secure Australia in a secure region'.

This outcome is separated into four program deliverables:

- ▶ **security intelligence analysis and advice**, including strategic, investigative and complex analysis, threat assessments, border security, critical infrastructure protection, contributing to policy development, and support to prosecutions;
- ▶ **protective security advice**, including counter-terrorism checking, personnel security, physical security, and contributing to policy development;
- ▶ **security intelligence investigations and capabilities**, including the maintenance and enhancement of all-source security intelligence collection, complex tactical and technical analysis, technical research and development, counter-terrorism response, national and international liaison, and contributing to policy development; and

- ▶ **foreign intelligence collection in Australia** at the request of the Minister for Foreign Affairs or the Minister for Defence, as well as incidentally through security intelligence capabilities.

ASIO has two key performance indicators:

- ▶ the contribution of ASIO's action and advice to the management and the reduction of risk to:
  - ▷ people and property;
  - ▷ government business and national infrastructure; and
  - ▷ special events of national and international significance; and
- ▶ the security of ASIO's activities.

Achievement against these indicators is monitored through the following mechanisms:

- ▶ the level of government satisfaction, as indicated by client feedback;
- ▶ relevant client feedback on agency outputs in regard to quality and timeliness;
- ▶ resource use against priorities and cost-effectiveness;
- ▶ ASIO's security performance; and
- ▶ maintenance of ASIO's security integrity.

ASIO undertakes a yearly Stakeholder Satisfaction Survey with key government partners. Details of this survey can be found on page 47.

Part 2 of the *ASIO report to parliament 2012–13* provides unclassified detail on ASIO's work and performance in relation to its key performance indicators.

## DELIVERABLE 1

Security intelligence analysis and advice informs stakeholders of ASIO's work in countering terrorism, espionage and other threats to national security. It includes:

- ▶ strategic assessment and advice;
- ▶ threat assessment and advice;
- ▶ industry engagement and advice;
- ▶ proscription-related advice;
- ▶ security assessment advice; and
- ▶ support to security intelligence-related prosecutions and litigation.

# Security intelligence analysis and advice

## Strategic assessment and advice

ASIO publishes a range of strategic assessments and advice which inform the priorities, policy development and decision-making of government agencies in the national security community, and more broadly. ASIO strategic assessments provide advice to the Australian government on key issues affecting the current security environment and future security outlook.

Strategic assessments also inform ASIO's various security assessment, counter-terrorism and counter-espionage functions; inform investigations and operations; provide environmental context; assist in the understanding of contemporary security issues; provide forewarning of potential emerging issues; and provide a basis for longer-term decision-making. ASIO strategic assessments are produced in response to Organisational requirements and requests from partner agencies.

## Performance 2012–13

ASIO produced strategic assessments on a diverse range of topics, addressing the implications for the security of Australia and Australian national interests abroad. Topics included developments in the security environments of Afghanistan, Syria and South-East Asia; the focus and leadership of key terrorist groups such as al-Qa'ida and emerging groups like Jabhat al-Nusra; thematic issues such as 'lone actor' extremists, indicators of radicalisation, extremism in Australian prisons, unauthorised maritime arrivals and people smuggling; and trends in foreign espionage activities in Australia.

In undertaking this work, ASIO continued to cooperate closely with other members of the Australian Intelligence Community and a range of partners including the Attorney-General's Department, the Department of the Prime Minister and Cabinet (PMC), the Department of Foreign Affairs and Trade (DFAT), the Department of Immigration and Citizenship (DIAC), the Australian Federal Police (AFP), the Australian Customs and Border Protection Service and other federal, state and territory government agencies.

## Threat assessment and advice

ASIO provides assessment and advice on threats to Australians and Australian interests from terrorism, violent protest, communal violence, espionage and foreign interference. ASIO provides this advice principally through threat assessments prepared by the National Threat Assessment Centre (NTAC).

NTAC, Australia's national authority for assessing threats to Australian interests

globally, brings together Australian government agencies to collect, monitor, collate and analyse all threat intelligence available to the Australian Government.

NTAC threat assessments provide clients with advice about actual or potential security threats to people, places or events to assist them to plan and implement risk mitigation strategies. The focus of these assessments includes threats to Australians, threats to Australian and overseas dignitaries, terrorist and protest threats to diplomatic premises in Australia, threats to critical infrastructure and resource sectors, and threats to major events. Threat assessments help DFAT formulate and disseminate overseas travel advice for Australians, and contribute to the protective security arrangements of government and industry.

NTAC's success in identifying, responding rapidly to, and reporting on specific and emerging threats lies in the ability of all seconded officers in NTAC to have reach-back into the resources of their originating agency. In addition to ASIO officers, NTAC has seconded officers from the following agencies:

- ▶ the Australian Federal Police;
- ▶ the Australian Secret Intelligence Service (ASIS);
- ▶ the Australian Signals Directorate (ASD) (also known as the Defence Signals Directorate or DSD);
- ▶ the Defence Intelligence Organisation (DIO);
- ▶ the Department of Foreign Affairs and Trade;
- ▶ the Department of Infrastructure and Transport;
- ▶ the Office of National Assessments (ONA); and
- ▶ the New South Wales Police Force.

## Performance 2012–13

In 2012–13 NTAC focused its assessment and advice on areas where it assessed Australians to be at greatest threat.

NTAC continued to leverage relationships with key international partners who also produce threat assessment products.

NTAC disseminated assessment and advice on terrorist threats to Australian interests overseas, including in countries affected by the Arab Spring and other conflicts, such as that in Syria. This advice materially contributed to the DFAT travel advisory and the consular assistance provided to Australians overseas. NTAC provided advice to the Australian government after the Boston Marathon bombings and the Woolwich attack and subsequently prepared further advice on the threat from ‘lone actors’ and potential threats from the release of extremist material, as well as threats to Australia’s defence assets.

NTAC disseminated advice to state and territory law enforcement agencies responsible for providing security responses and ensuring public order during protests. Emotive issues such as the Syrian and Egyptian conflicts drew protests and counter-protests, and early indications of the intent and capability of the protesters were key to ensuring appropriate security measures were employed.

In 2012–13 NTAC prepared threat assessment advice to inform the protective security measures for a range of special events, including the 43<sup>rd</sup> Pacific Islands Forum, the 10<sup>th</sup> anniversary of the Bali bombing, ANZAC Day commemorations in Turkey and France, and the London Olympic and Paralympic Games. NTAC also produced assessments to inform security-planning decisions related to G20 events in 2014.

## Industry engagement and advice

### Critical infrastructure

ASIO provides advice to industry to help protect Australia’s critical infrastructure, including in the banking and finance, communications, energy and health sectors. ASIO engages directly with industry partners to provide relevant, timely and accurate advice to inform them of current threats and identify existing vulnerabilities.

### Cyber

The threat posed by malicious activity conducted by cyber means has continued to increase due to a more interconnected society. ASIO provides security advice to industry partners on the threat posed by cyber espionage to sensitive information, including intellectual property, and personal particulars of staff or customers. In the reporting period, ASIO created new and maintained existing productive relationships with private businesses to assist them mitigate these cyber threats.

Increasingly ASIO cooperates with the private sector on cyber security issues. This is conducted in partnership with ASD and CERT Australia.

## Business Liaison Unit

The Business Liaison Unit (BLU) is another way ASIO provides a direct public interface between the Australian Intelligence Community and Australian business.

The BLU equips corporate security managers with credible, intelligence-backed reporting that enables them authoritatively to brief executive management and staff and to enhance their risk management and continuity planning. The BLU does this by producing and disseminating domestic and international security information and by actively engaging with Australian businesses, particularly through attendance and engagement at key industry forums.

The BLU also regularly produces an unclassified bulletin for all subscribers. This resource informs Australian security managers about current and emerging issues and the range of ASIO information available to them.

### Performance 2012–13

In 2012–13 the BLU conducted 186 separate meetings with corporate security and risk managers in every state and territory in Australia, providing specific security advice and information on the full range of services and support offered by the BLU.

The BLU published 105 reports on its subscriber-based website, including 26 reports from foreign liaison counterparts and 19 reports from other Australian government agencies.

In addition, the BLU hosted two dedicated security briefing days for corporate security managers from the oil and gas, and banking and finance sectors.

[www.blu.asio.gov.au](http://www.blu.asio.gov.au)



## Proscription-related advice

ASIO contributes to the process for proscription under the *Criminal Code Act 1995* by providing advice on organisations to the Attorney-General's Department to inform the Attorney-General's decision-making process. ASIO provides this advice in the form of an unclassified statement of reasons, which is prepared in consultation with DFAT, the Attorney-General's Department and the Australian Government Solicitor.

The Australian Government had proscribed 18 organisations as at 30 June 2013:

1. Abu Sayyaf Group;
2. al-Qa'ida;
3. al-Qa'ida in Iraq;
4. al-Qa'ida in the Lands of the Islamic Maghreb;
5. al-Qa'ida in the Arabian Peninsula;
6. al-Shabaab;
7. Ansar al-Islam (formerly known as Ansar al-Sunna);
8. Hamas's Izz al-Din al-Qassam Brigades;

9. Hizballah's External Security Organisation;
10. Islamic Movement of Uzbekistan;
11. Jabhat al-Nusra;
12. Jaish-e-Mohammad;
13. Jamiat ul-Ansar;
14. Jemaah Islamiyah;
15. Kurdistan Workers' Party;
16. Lashkar-e Jhangvi;
17. Lashkar-e-Tayyiba;
18. Palestinian Islamic Jihad.

### Performance 2012–13

During the reporting period, ASIO provided proscription-related advice to the Attorney-General on the terrorism-related activities of six groups. In 2012–13 the Attorney-General re-listed five groups—al-Shabaab, Hamas's Izz al-Din al-Qassam Brigades, the Kurdistan Workers' Party, Lashkar-e-Tayyiba and Palestinian Islamic Jihad—and listed Jabhat al-Nusra for the first time.

### Security assessment advice

ASIO's security assessment function is an important component of Australia's national security arrangements. It provides a mechanism for security to be considered by government agencies when taking certain actions—those defined as 'prescribed administrative actions' in the ASIO Act. Examples include issuing passports, granting visas, granting access to sensitive government information (security clearances) and granting access to restricted areas such as ports and airports and sensitive goods such as ammonium nitrate.

Most ASIO security assessments are made at the request of another department or agency, although ASIO can issue assessments as a consequence of an ASIO intelligence investigation. Security assessments can range from a check of personal details against ASIO's intelligence holdings to an in-depth intelligence investigation to determine the nature and extent of a threat.

Security assessments only consider factors related to 'security'. Security assessments are not character checks; factors such as criminal history, dishonesty or deceit are only relevant to ASIO's advice if they have a bearing on security considerations.

Upon making a security assessment, ASIO may provide:

- ▶ **non-prejudicial advice**, which means ASIO has no security-related concerns about the proposed 'prescribed administrative action';
- ▶ **a qualified assessment**, which generally means ASIO has identified information relevant to security which the government agency may seek to use in making its decision, but ASIO does not make a recommendation in relation to the 'prescribed administrative action'; or
- ▶ **an adverse assessment**, in which ASIO recommends a prescribed administrative action be taken, such as cancelling a passport or declining access to a security-controlled area.

The consequences of an ASIO security assessment depend on the purpose for which it is made and the associated legislation, regulation or policy. In some cases, decision-makers are obliged to take action, or are prevented from taking action, because of an ASIO security assessment.

In other cases, the ASIO assessment is considered by the decision-maker among a range of other factors.

### Appeal mechanisms for security assessments

Where ASIO provides an Australian government agency with an adverse or qualified security assessment on an individual, the agency concerned is generally required to notify the subject within 14 days. For most categories of security assessment, merits review is available in the Security Appeals Division of the Administrative Appeals Tribunal (AAT). The AAT may inform itself on any matter in such manner as it considers appropriate.

For a defined range of cases, the Independent Reviewer of Adverse Security Assessments (see page 39) has conducted reviews of individuals who have received adverse security assessments from ASIO and remain in immigration detention.

The Inspector-General of Intelligence and Security (IGIS) maintains a close interest in ASIO's security assessments. It is not a function of the IGIS to review the merits of adverse assessments, but the IGIS may, under the *Inspector-General of Intelligence and Security Act 1986*, review the legality and propriety of associated ASIO practices and procedures.

Judicial review regarding the processes used by ASIO in making a security assessment is possible through the Federal Court and the High Court of Australia.



### Passports

Under the *Australian Passports Act 2005*, ASIO may request on security grounds that an Australian passport be cancelled or an application for an Australian passport be declined. Withholding passports is an important means of preventing Australians from travelling overseas to engage in activities prejudicial to national security—for example, to train, support or participate in terrorism. It may also be used to help prevent an Australian already overseas from participating—or further participating—in activities that are prejudicial to the security of Australia or another country.

### Performance 2012–13

During the reporting period, ASIO issued adverse security assessments in respect of 18 passports.



## Citizenship

Under the *Australian Citizenship Act 2007*, the Minister for Immigration and Citizenship may not approve the granting of Australian citizenship where ASIO has made an adverse security assessment in relation to an applicant.

## Performance 2012–13

In 2012–13 ASIO issued one adverse security assessment in relation to a citizenship application.

## Visa security assessments

Australia's border security is layered. DIAC uses a number of systems and databases to detect persons of interest. Ongoing checks are performed at different times through the traveller pathway including referral to ASIO.

In most visa categories, a visa may not be issued—or may be cancelled—where ASIO determines the applicant to be directly or indirectly a risk to 'security' as defined in the ASIO Act.

Separate to visa application referrals from DIAC, ASIO's security intelligence investigations can identify the holder of a valid visa to Australia as a risk to Australia's security. In such circumstances, ASIO may issue an adverse security assessment, and the visa may then be cancelled, irrespective of whether the individual is already in Australia or is yet to travel.

## Performance 2012–13

Table 1

Type of entry	Number of assessments completed 2011–12	Number of assessments completed 2012–13
Temporary visas	12 623	18 748
Permanent visas	5708	3681
Onshore protection (Air)	319	257
Offshore refugee / humanitarian	687	3369
Unauthorised maritime arrivals	4760	3394
<b>TOTAL</b>	<b>24 097</b>	<b>29 449</b>

The increased number of security assessments for offshore refugee / humanitarian visas (see Table 1) reflects the recommendations of the Report of the Expert Panel on Asylum Seekers, the Houston Review. The report recommended increasing Australian's humanitarian program to 20 000 places per annum, including a minimum 12 000 places allocated for the refugee component.

### Counter-terrorism security assessments

Individuals likely to require access to sensitive air and maritime port areas must undergo appropriate background checking—including security checking—before being granted Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC) permitting such access.

ASIO's role in the ASIC and MSIC process is primarily to consider any terrorism concerns about those seeking access. AusCheck, located within the Attorney-General's Department, coordinates the larger suite of background checks, including criminal history checks, and assesses an applicant's overall suitability to hold an ASIC or MSIC. ASIO may recommend against an ASIC or MSIC if there are security concerns.

ASIO provides, via the AFP, counter-terrorism background checks as part of the licensing process by Australian states and territories for access to security-sensitive ammonium nitrates (SSANs), which are used as an explosive, particularly by the mining industry, and as a fertiliser in agriculture. Each state and territory has its own licensing regime, consistent with a set of principles agreed in 2005 by the Council of Australian Governments (COAG).

Similar ASIO checks are provided for those requiring access to security-sensitive biological agents (SSBA) as part of the SSBA Regulatory Scheme flowing from the *National Health Security Act 2007*. ASIO may recommend against a licence for access to SSANs or SSBAs.

ASIO also provides, via the AFP, security assessment advice on any terrorism concerns for individuals requiring access to the Australian Nuclear Science and Technology Organisation nuclear facility at Lucas Heights, New South Wales (NSW).

ASIO security assessment advice is also provided for some special-event accreditation, such as the G20 meetings in Australia in 2014.

### Performance 2012–13

In 2012–13 ASIO completed 130 045 counter-terrorism security assessments. No adverse or qualified counter-terrorism security assessments were issued.

### Personnel security assessments

The Protective Security Policy Framework (PSPF) sets out Australian government policy and guidance on protective security, including policy for the granting of clearances for access to national security classified information. In almost all circumstances, a department or agency must request security assessment advice from ASIO as part of its overall consideration of whether or not to grant a national security clearance.

Except for ASIO officers—and, in a limited number of additional cases, where ASIO is the clearance sponsor—ASIO is not the issuing authority for personnel security clearances and it is up to individual departments and agencies to form a decision, taking into account ASIO’s advice. From 1 October 2010 all Australian government security checks—with the exception of a few exempt agencies—were consolidated under a single security vetting service, the Australian Government Security Vetting Agency (AGSVA). AGSVA is located in the Department of Defence and is ASIO’s primary client for security assessments in relation to national security clearances.

## Performance 2012–13

Table 2

Type of access	Assessments completed 2012–13
Top Secret	
Positive Vetting	1789
Negative Vetting Level 2	6625
Negative Vetting Level 1	19 168
Other	4
<b>Total</b>	<b>27 586</b>

## Support to security intelligence-related prosecutions and litigation

In 2012–13 ASIO was involved in litigation matters including terrorism and other criminal prosecutions, civil matters in which ASIO material was sought as evidence, and judicial and administrative review of ASIO security assessments. The recent increase in security assessment litigation—in particular, relating to unauthorised maritime arrivals—and complex litigation matters involving multiple Commonwealth agencies required significant legal resources.

ASIO’s focus remained the protection of sensitive national security information while engaging in civil and criminal matters, and the administrative and judicial review of decisions by ASIO and other agencies.

### Performance 2012–13

In 2012–13 ASIO was involved in approximately 50 litigation matters. A snapshot of cases covering support to criminal prosecutions, and other civil matters, is outlined below.

#### *M47/2012 v. Director-General of Security and Others [2012] HCA 46*

M47, an unauthorised maritime arrival on the *Oceanic Viking* vessel, asked the High Court to quash his adverse security assessment on the basis that ASIO had denied him procedural fairness in not interviewing him.

M47 also sought an order that a visa be granted and a declaration that his immigration detention was unlawful. M47 instituted proceedings in the High Court against five defendants, including the Director-General of Security.

On 5 October 2012 the High Court delivered its judgement, finding ASIO had provided procedural fairness in the circumstances of the case. On 29 November 2012 the court remitted M47's visa application to the Refugee Review Tribunal for further consideration.

### *S138/2012 v. Director-General of Security and Others*

In 2009 ASIO issued an adverse security assessment in respect of S138, an unauthorised maritime arrival in immigration detention. S138 asked the High Court to quash the assessment, compel a visa grant and declare his detention unlawful. In 2012 the court handed down its related M47 decision, which was limited to applicants who had made valid protection visa applications under Migration Regulation 866.225(a). S138 did not fall into this category because he was not eligible to make a valid visa application and had requested the Minister for Immigration and Citizenship exercise his discretion to enable him to do so. This request was declined.

On 7 June 2013, following an advisory opinion by the Independent Reviewer of Adverse Security Assessments, the Director-General issued a non-prejudicial security assessment for S138. DIAC subsequently granted a bridging visa pending consideration of S138's refugee claim. On 13 June 2013, on the basis of the parties' consent, the court dismissed the application.

### *The Queen v. Khazaal [2012] HCA 26*

Mr Khazaal was found guilty in 2008 of making a document in connection with a terrorist act and sentenced to 12 years imprisonment. The jury was unable to reach a verdict on the additional charge of attempting to incite others to commit a terrorist act. In 2011 the New South Wales Court of Criminal Appeal (NSW CCA) overturned the conviction and ordered a retrial, to be heard with the incitement retrial. The Crown was granted special leave to appeal to the High Court, on the basis of provisions in the *Criminal Code Act 1995* relating to evidence.

On 10 August 2012 the High Court unanimously allowed the appeal of the Commonwealth Director of Public Prosecutions, overturning the NSW CCA decision and reinstating the conviction. The court remitted the matter to the NSW CCA to consider Mr Khazaal's sentence appeal. On 13 June 2013 the NSW CCA dismissed Mr Khazaal's appeal against the severity of his sentence. Mr Khazaal may be eligible for release on parole in 2017.

### *RJCG v. Director-General of Security [2013] FCA 269*

ASIO assessed the applicant, an Australian citizen employed by the Commonwealth, to have engaged in acts of foreign interference by providing information to foreign intelligence officers. ASIO issued an adverse security assessment recommending revocation of the applicant's security clearance.

On 22 August 2012 the AAT affirmed ASIO's decision. The applicant appealed this decision to the Federal Court, which will hear the matter in November 2013.

*TCXG and Director-General of Security and Anor [2013] AATA 284*

On 21 June 2012 ASIO issued an adverse security assessment in respect of TCXG, and the Minister for Foreign Affairs consequently refused TCXG's application for an Australian passport. ASIO assessed that the applicant adhered to an extremist interpretation of Islam which condoned the use of politically motivated violence. ASIO assessed that TCXG's extremist actions involved encouraging, fostering and supporting extremist activities, including the use of politically motivated violence. On 10 May 2013 the AAT affirmed ASIO's 2012 adverse security assessment and DFAT's passport refusal.

*NBMW v. Minister for Immigration and Citizenship [2013] FCA 651*

The applicant, an unauthorised maritime arrival, challenged the ASIO adverse security assessment. On 12 September 2012 the AAT affirmed the security assessment. The applicant appealed this decision to the Federal Court but then discontinued that appeal and sought instead to join the Director-General to the separate Federal Court action against the Minister for Immigration and Citizenship. The applicant claimed the security assessment was not lawful or validly made because ASIO had denied NBMW procedural fairness.

On 5 July 2013 the Federal Court dismissed the application to join the Director-General to the separate proceedings.

## DELIVERABLE 2

Protective security advice enhances physical, technical, procedural, personnel and information security. It includes:

- ▶ protective security risk reviews;
- ▶ Top Secret certifications;
- ▶ technical surveillance countermeasures;
- ▶ security equipment evaluation;
- ▶ protective security training; and
- ▶ the Protective Security Policy Framework.

# Protective security advice

ASIO T4 Protective Security provides advice to the Australian government on protective security in Australia. ASIO also provides protective security advice to state and territory governments and Australian businesses, with approval from the Attorney-General.

T4's role derives from section 17(1)(d) of the ASIO Act; unlike other parts of the Act, this section does not limit ASIO's advice to matters defined by 'security'. In practice, however, much of T4's advice is directed towards risks relating to the threats of terrorism, issue-motivated groups, espionage and foreign interference.

**UNCLASSIFIED**

 Australian Government  
Australian Security Intelligence Organisation

### Protective security and ASIO-T4

**What is T4?**

The T4 section with the Australian Security Intelligence Organisation focuses on securing human, information and physical resources. ASIO-T4 is the primary body with the responsibility to provide protective security advice to Ministers, authorities of the Australian Government and other persons determined by the Attorney-General.

T4's services are utilised extensively by the Australian Government, and selectively by state and territory governments such as for special events and critical infrastructure and the private sector. T4 maintains a purpose-built facility to carry out training, testing, and some certification tasks.

**The basis of T4's activities**

T4's activities are derived from paragraph 17(1)(d) of the Australian Security Intelligence Organisation Act. This paragraph does not limit ASIO's protective security advice responsibilities to matters contained within the definition of 'security' in section 4 of the ASIO Act. This sub-section was added to ASIO's legislative functions in 1986 as a response to recommendations by the Hope Royal Commission into Australian Security and Intelligence Agencies, recognising the broader utility of the protective security advice that ASIO can provide.

In practice, the vast majority of T4's advice is directed towards protection from espionage, sabotage and politically motivated violence.

As part of ASIO's Protective Security Branch, T4 provides independent evaluation of the adequacy and efficacy of the security of Australian Government departments and agencies, provides advice on protective security risks and countermeasures, and evaluates security products for government use. In line with a determination of the Council of Australian Governments, T4 undertakes bilateral protective security risk reviews of ' vital' critical infrastructure. It also, under the authority of the Australian Government Protective Security Manual, is a certification authority for premises handling Top Secret material, and conducts Technical Surveillance Countermeasures (sweeping) services.

As part of ASIO, T4 is able to draw extensively upon the raw and assessed security intelligence from ASIO intelligence sources – both domestic and international – and to leverage sensitive technical partnerships with close foreign partners. This allows T4 to provide high quality, confidential advice and timely intelligence-led advice compared to similar bodies without access to such information. T4 works closely with ASIO's National Threat Assessment Centre and Critical Infrastructure Protection Directorate.

**T4's protective security advice**

T4 provides protective security advice to clients on a cost-recovery basis. Advice to state and territory governments and private sector clients is provided on the same basis with approval from the Attorney-General.

T4's protective security advice largely comprises:

- Functional recommendations directed towards achieving operational security objectives consistent with the requirements of the Protective Security Manual and/or mitigating security vulnerabilities and risks – such as in the case of reasonably vital critical infrastructure. These recommendations may address any number of physical, personnel, information or administrative risks.
- Inspection and certification of the physical security of sites in Australia handling Top Secret material.
- Technical surveillance countermeasures testing within Australia (sweeping).

Clients typically use T4 security recommendations as the basis to engage private industry security consultants to

 [www.asio.gov.au](http://www.asio.gov.au) **UNCLASSIFIED**

## WHY IS IT CALLED T4?

Previously, ASIO had a specific unit which dealt with a range of technical issues—it was then known as 'T' Branch. The fourth group within this technical unit focused on protective security and was known as T4. Although the branch no longer exists as such, the term T4 became so widely recognised across the Australian government and industry that it has been retained by ASIO and is still in use today.

## Protective security risk reviews

One of T4's highest priorities is providing protective security risk reviews (PSRRs) for Australian government vital and critical infrastructure assets. T4 also provides vulnerability assessments to clients. These assessments identify weaknesses in protective security arrangements and provide practical recommendations to address the identified vulnerabilities.

T4 also provides protective security advice to providers of shared internet gateways used by Australian government agencies and, on behalf of the Security Construction and Equipment Committee, undertakes physical security inspections of couriers and external destruction services.

### Performance 2012–13

In 2012–13 T4 completed three PSRRs and/or vulnerability assessments and 10 physical security inspections, including external destruction services and shared internet gateway facilities.

## Top Secret certifications

T4 is the Australian government's physical security certifying authority for Zone 5 (Top Secret) facilities within Australia. T4 also certifies the physical security of sensitive compartmented information facilities on behalf of Defence Intelligence Security (DIS), which is the accrediting authority. DIS sits within the Defence Intelligence and Security Group of the Department of Defence and is the security provider for the Defence intelligence agencies. Re-certification of Zone 5 facilities is required every five years.

### Performance 2012–13

In 2012–13 T4 completed the Zone 5 certification of 34 sites. This included undertaking 83 physical security inspections during the reporting period.

## Technical surveillance countermeasures

T4 offers assistance in technical surveillance countermeasures assistance to Australian government departments and agencies to provide a level of assurance that highly classified or sensitive discussions and information are not subject to compromise through technical means. Inspections include electronic surveys, monitoring of premises for possible covert electronic activity, and physical security inspections.

### Performance 2012–13

For reasons of national security, ASIO's performance in relation to this activity is not covered in this report.

## Security equipment evaluation

The Security Construction and Equipment Committee (SCEC) is the standing interdepartmental committee responsible for the evaluation and approval of security equipment used by Australian government departments and agencies. SCEC is chaired by a senior ASIO officer and reports directly to the Protective Security Policy Committee, which is tasked with developing and publishing guidelines for the protection of Australian government resources.

### Performance 2012–13

In 2012–13 T4 delivered 10 SCEC locksmith courses, four SCEC security zone consultant courses and one container maintenance course.

As part of the SCEC testing program, T4 completed 29 security equipment product evaluations, published 18 security equipment guides and commenced re-evaluating all product categories for inclusion in the new Security Equipment Evaluation Products List (SEEPL) catalogue. As approved at the May 2013 SCEC meeting, T4 has implemented a rolling program to open each product category in the SEEPL to new applications. Six product categories are opened to applications on a quarterly basis in preparation for the planned release of the SEEPL in late 2014.

## Protective security training

T4 conducts a range of training courses for Australian government agencies and their staff, commercial security consultants and locksmiths as part of the requirements for SCEC endorsement and approval.

The security practitioner's course provides training in the practical application of protective security for officers employed as agency security advisers or defence security officers within Australian government departments.

### Performance 2012–13

In 2012–13 T4 delivered four agency security adviser courses and six courses for the Attorney-General's Department's Protective Security Training Centre.

## Protective Security Policy Framework

The Australian government's PSPF provides guidance and establishes minimum standards to be applied by all Australian government departments and agencies in regard to the physical security of a site, including the handling, storage and processing of sensitive and classified information.

T4 produces a series of *Technical Notes*, which provide detailed interpretations of the PSPF standards in relation to protective security issues. These documents are available to government departments and agencies.

ASIO also makes a significant contribution to the development of protective security policy through its involvement in the Protective Security Policy Committee and the Inter Agency Security Forum.



### DELIVERABLE 3

Security intelligence investigations and capabilities fulfil ASIO's intelligence collection requirements through all-source security intelligence collection, complex tactical investigations, analysis, and engagement with national and international partners. It includes:

- ▶ counter-terrorism investigations and analysis;
- ▶ counter-espionage and foreign interference investigations and analysis; and
- ▶ border integrity investigations and analysis.

## Security intelligence investigations and capabilities

### Counter-terrorism investigations and analysis

The threat of terrorism to Australia and its interests is real. Terrorism has become a persistent feature of Australia's security environment. It threatens Australians and Australian interests both at home and overseas.

ASIO's Counter Terrorism Division conducts counter-terrorism investigations and operations to identify and mitigate harm from individuals and groups engaged in a range of extremist and terrorism-related activities. This includes individuals planning violence in Australia, seeking to travel overseas for terrorism, and recruiting, facilitating and radicalising others.

#### Performance 2012–13

ASIO's performance in relation to its counter-terrorism investigations and operations are reported on only in the classified Part 3 of the annual report for reasons of national security.



The Counter Terrorism Control Centre (CTCC) was established in 2010 to set and manage counter-terrorism priorities, identify intelligence requirements and ensure the processes of collecting and distributing counter-terrorism information are fully harmonised and effective across the spectrum of Australia's counter-terrorism activities. The multi-agency centre is headed by a senior ASIO officer. It has senior-level representation from across the national security community.

In 2012–13 the CTCC produced an updated *Counter-Terrorism Intelligence Planning Document* and published its *Annual Evaluation Report*.

Together, these classified documents provide a framework to set priorities for and evaluate the national security community's performance against agreed benchmarks.

The CTCC publishes a classified Monthly Counter-Terrorism Priorities statement, which provides relevant agencies with advice on the most immediate counter-terrorism threats and the investigations, operations or issues requiring the most immediate focus. This allows for the efficient coordination of counter-terrorism resources and priorities across the Australian Intelligence Community.

## Counter-espionage and foreign interference investigations and analysis

Espionage and foreign interference activities against Australia and Australian interests pose significant threats and have the potential to damage Australia, its people and its interests, including defence, intelligence, scientific and technical capabilities; our trade and the economy; and international relations. Such activities may also pose a threat to the welfare of individual Australians through coercion or threatened violence.

ASIO's Counter Espionage and Interference Division is committed to discovering, defending against, and degrading espionage and foreign interference activities directed against Australia and Australian interests. ASIO works closely with partners across government and industry to heighten awareness of the threat environment and to drive and shape appropriate security policy responses.

## Performance 2012–13

ASIO's performance in relation to its counter-espionage and foreign interference investigations and operations are reported on only in the classified Part 3 of the annual report for reasons of national security.

## Contact Reporting Scheme

The Contact Reporting Scheme (CRS), managed by ASIO under the PSPF, is an effective tool to identify foreign intelligence service activity directed towards the cultivation and recruitment of Australian government employees. Under the CRS, all government employees are obliged to report contact which appears to be suspicious, ongoing, unusual or persistent in any respect. This contact could be either official or social, with foreign nationals either in or outside Australia.

The CRS assists ASIO to identify intelligence or hostile activity directed against Australia and its interests, government employees and contractors, and people who hold an Australian government security clearance. It helps identify trends, including the type of information of interest to foreign intelligence services, who is interested in it, and the methods foreign intelligence

services are prepared to use to collect it. ASIO uses this intelligence to assist in the formulation of threat assessment and security intelligence advice.

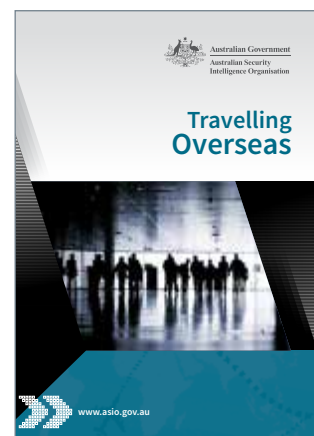
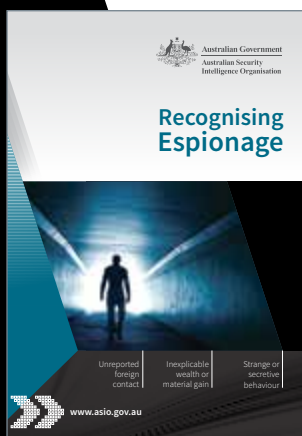
## Performance 2012–13

In the reporting period the CRS received and evaluated reports submitted through the scheme. In May 2013 ASIO hosted a conference to provide agency security advisers with the latest threat information and to share information and experiences in relation to this threat.

The CRS team also produced a suite of new unclassified resources (see below) to assist Australian government agency employees with advice about foreign intelligence service threats and the reporting mechanisms available.

## Border integrity investigations and analysis

ASIO identifies, investigates and provides advice on serious threats to Australia's border integrity, with a focus on maritime people smuggling as part of the whole-of-government framework to combat people smuggling activities.



## Performance 2012–13

ASIO's outcomes in relation to its border integrity investigations and operations are reported on only in the classified Part 3 of the annual report for reasons of national security.

## National counter-terrorism responsibilities

Australia's national strategic approach to countering terrorism requires a multi-layered and collaborative approach based on strong relationships between government, private industry, members of the community and international partners. As a member of the Australia and New Zealand Counter-Terrorism Committee (ANZCTC, formerly the National Counter-Terrorism Committee), ASIO contributes actively to these counter-terrorism arrangements.

The ANZCTC was established by the Intergovernmental Agreement on Australia's National Counter-Terrorism Arrangements to:

- ▶ provide strategic and policy advice to heads of government and relevant ministers;
- ▶ coordinate an effective nationwide counter-terrorism capability;
- ▶ maintain effective arrangements for sharing appropriate intelligence and information between all relevant agencies in all jurisdictions;
- ▶ provide advice in relation to the administration of ANZCTC funds; and
- ▶ maintain the National Counter-Terrorism Plan and associated documentation.

## National counter-terrorism exercises

ASIO also contributes to the national counter-terrorism exercise program. These exercises bring together Commonwealth and state/territory governments, law enforcement agencies, intelligence agencies and emergency management agencies to test and improve response arrangements across jurisdictions and organisations.

ASIO is also participating in the Australian Government preparation for the G20 summit, including an interagency and multi-jurisdictional exercise program to ensure readiness for the event.

## Performance 2012–13

ASIO participated in a number of national counter-terrorism exercises including:

- ▶ a nationwide series of exercises designed to test interoperability between the AFP, ASIO, state and territory police and the Commonwealth Director of Public Prosecutions;
- ▶ a series of exercises to simulate local and national counter-terrorism responses to a terrorist attack on an Australian critical infrastructure site; and
- ▶ a number of small-scale discussion exercises held in Queensland and Victoria aimed at enhancing multi-agency interoperability and decision-making.

During these exercises, ASIO tested interoperability in a multi-agency environment, particularly intelligence arrangements and information flows.

## DELIVERABLE 4

Foreign intelligence collection in Australia includes tasks undertaken at the request of the Minister for Defence or the Minister for Foreign Affairs.

# Foreign intelligence collection in Australia

ASIO has a statutory function, under section 17(1)(e) of the ASIO Act, to obtain foreign intelligence in Australia.

ASIO exercises its foreign intelligence collection powers where authorised by the Attorney-General, in relation to matters that are in the interests of Australia's national security, Australia's foreign relations or Australia's national economic wellbeing. ASIO completes this activity in close cooperation with foreign intelligence collection partners—ASIS and ASD.

## Performance 2012–13

At the request of the Minister for Foreign Affairs or the Minister for Defence, ASIO has used its special collection powers to undertake foreign intelligence collection within Australia on issues of very high national significance. ASIO's performance in relation to this intelligence collection activity is measured by stakeholders in terms of ASIO meeting the intelligence requirements of the sponsoring agency, and also the National Intelligence Priorities set by the National Security Committee of Cabinet.

For reasons of national security, ASIO's outcomes in relation to its foreign intelligence collection operations are reported on only in the classified Part 3 of the annual report.





# Part 3

## OUTCOMES AND HIGHLIGHTS

‘An increasing focus for ASIO in recent years has been the use of the internet as a tool covertly to extract sensitive, private or classified information for the purpose of espionage, political or diplomatic advantage, or commercial gain.’

► *Speech by the Director-General to the Biennial Conference of the District and County Court Judges [of Australia and New Zealand]  
26 June 2013*





## PART 3 EXCLUSION

The Attorney-General has approved the exclusion of Part 3 in its entirety from the unclassified ASIO report to parliament for reasons of national security.





# Part 4

## ASIO AND ACCOUNTABILITY

‘The ever-changing security environment means the laws within which security agencies operate must continue to modernise to reflect the level and nature of emerging threats to our nation.’

► *Speech by the Director-General to the Biennial Conference of the District and County Court Judges [of Australia and New Zealand]  
26 June 2013*

## Attorney-General

---

ASIO is responsible to the Australian government through the Attorney-General, as outlined in the ASIO Act. The Hon. Mark Dreyfus QC MP was sworn in as Attorney-General on 4 February 2013, replacing the Hon. Nicola Roxon MP.

ASIO informs the Attorney-General of significant national security developments. During the reporting period, ASIO provided advice to the Attorney-General on a range of issues connected to the security environment, specific investigations and operations, and administrative matters relevant to ASIO, primarily communicated through over 300 submissions.

ASIO's operational activity is conducted in accordance with the *Attorney-General's guidelines*, last updated by the Attorney-General on 10 December 2007 under sections 8A(1) and 8A(2) of the ASIO Act. The *Guidelines* stipulate that ASIO's information collection activities should be conducted in a lawful, timely and efficient manner, using the least intrusion necessary into an individual's privacy.

All ASIO warrants (other than questioning and detention warrants, which are issued and approved by a person as specified under Part III, Division 3 of the ASIO Act) are issued by the Attorney-General after consideration of a request presented by the Director-General of Security. For every warrant raised, ASIO is required to report to the Attorney-General on the extent to which action undertaken in respect of the warrant assisted the Organisation in carrying out its functions.

## Parliamentary oversight

---

### Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is appointed under section 28 of the *Intelligence Services Act 2001* (the ISA). The functions of the PJCIS are to:

- ▶ review the administration and expenditure of the Australian Intelligence Community, including the annual financial statements of these agencies;
- ▶ review any matter in relation to these agencies referred to the PJCIS by the responsible minister or a resolution of either House of the Commonwealth Parliament;
- ▶ review, as soon as possible after the third anniversary of the day on which the *Security Legislation Amendment (Terrorism) Act 2002* received royal assent, the operation, effectiveness and implications of amendments made by that Act, as well as the *Border Security Legislation Amendment Act 2002*, the *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* and the *Suppression of the Financing of Terrorism Act 2002*;
- ▶ review, by 22 January 2016, the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act; and
- ▶ report comments and recommendations from the PJCIS to each House of the parliament and to the responsible minister.

Under section 102.1A of the Criminal Code, the committee may also review the listing of organisations as proscribed terrorist organisations.

To assist the PJCIS review of administration and expenditure, ASIO provides a classified and an unclassified report each financial year and attends closed hearings.

### **PJCIS review of national security legislation**

In April 2012 the Attorney-General referred a national security legislation consultation package to the PJCIS for consideration and consultation.

The package sought to ensure the statutory powers accorded to Australia's intelligence and law enforcement agencies remained effective in the current and future national security environments. The submission had three components:

- ▶ **Telecommunications interception reform**, including proposals to modernise lawful access to communications and associated communications data under the *Telecommunications (Interception and Access) Act 1979*;
- ▶ **Telecommunications sector security reform**, including measures to mitigate the national security risks posed to Australia's telecommunications infrastructure; and
- ▶ **Australian Intelligence Community legislative reform**, proposing amendments to the ASIO Act and the ISA to improve the operational efficiency of intelligence agencies, as well as making some technical and administrative amendments.

ASIO prepared a classified and unclassified submission, which assisted the PJCIS's consideration of the issues. The Director-General attended two private hearings, on 29 October 2012 and 2 November 2012, to supplement these submissions.

The PJCIS tabled its findings on 24 June 2013, and these are still under consideration by the government. ASIO will continue to work with the Attorney-General's Department to inform the government's response to the review during 2013–14.

### **Senate Standing Committee on Legal and Constitutional Affairs**

Senate Estimates provides an opportunity for parliamentary scrutiny of the executive branch of government, including on issues of departmental expenditure and government operations. As part of the Attorney-General's portfolio, ASIO appears before the Senate Standing Committee on Legal and Constitutional Affairs. In 2012–13, the Director-General and the Deputy Director-General, Capability Assessments and Coordination, appeared at Supplementary Budget Estimates, in October 2012, and Budget Estimates, in May 2013.

ASIO responded to questions on a broad range of topics during these hearings and through questions on notice.

Topics included:

- ▶ staffing and budget;
- ▶ proposed changes to national security legislation;
- ▶ security assessments;
- ▶ unauthorised maritime arrivals; and
- ▶ cyber security.

## Inspector-General of Intelligence and Security

---

The Office of the IGIS was formally established under the *Inspector-General of Intelligence and Security Act 1986*.

The IGIS, Dr Vivienne Thom, is an independent statutory office holder who is responsible for reviewing the activities of the Australian Intelligence Community to ensure the agencies act legally, with propriety, in compliance with ministerial guidelines and directives, and with due regard for human rights.

The IGIS conducts regular and ongoing inspections and monitoring of ASIO activities. The IGIS has wide-ranging powers similar to those of a royal commission, including access to ASIO records or premises at any time.

### Inquiry into asylum seekers presenting complex security issues

On 5 June 2013 the then Prime Minister, the Hon. Julia Gillard MP, requested that the IGIS conduct an inquiry into the management by Australian agencies of people seeking asylum who present complex security issues, particularly an Egyptian unauthorised maritime arrival who was the subject of an Interpol red notice. At the time of publishing this inquiry was ongoing.

# Independent Reviewer of Adverse Security Assessments

---

On 3 December 2012 the Hon. Margaret Stone commenced as the Independent Reviewer of Adverse Security Assessments (the Independent Reviewer).

The role of the Independent Reviewer is to conduct an independent advisory review of ASIO adverse security assessments furnished to DIAC in relation to individuals who remain in immigration detention, having been found by DIAC:

- ▶ to be owed protection obligations under international law; and
- ▶ to be ineligible for a permanent protection visa, or who have had their permanent protection visa cancelled, because they are the subject of an adverse security assessment.

In performing her role, the Independent Reviewer is required to:

- ▶ examine all material relied on by ASIO in making the adverse security assessment;
- ▶ provide an opinion to the Director-General as to whether the adverse security assessment is an appropriate outcome based on that and other relevant material; and
- ▶ make recommendations accordingly, for the Director-General's consideration.

The Independent Reviewer's Terms of Reference require her to conduct a periodic review of adverse security assessments for eligible persons every 12 months.

Immediately following her commencement, the Independent Reviewer informed eligible persons about their right to seek review and invited them to apply. All 55 eligible persons subsequently applied for review, and each is legally represented.

Between January and April 2013 ASIO provided the Independent Reviewer with 55 unclassified written summaries of the reasons for each of the adverse security assessments. The summaries were then forwarded to the applicants' legal representatives. These documents summarise, to the extent possible without prejudicing security, the basis for ASIO's decision to issue an adverse security assessment in respect of the individual. A process of receiving written submissions and hearing oral submissions from applicants has taken place since that time.

Where a submission from an eligible person contains new information or claims, the Independent Reviewer refers this information to ASIO for consideration before the review process proceeds.

In May 2013 the review of one of the 55 individuals ceased when ASIO issued a new non-prejudicial security assessment. This outcome was part of ASIO's own processes in respect of individuals who are the subject of an adverse security assessment and was not as a result of the independent review process.

In 2012–13 ASIO provided the Independent Reviewer with the information it had relied on in making the adverse security assessments for all eligible persons. Shortly after the Independent Reviewer's appointment, ASIO advised it was reconsidering the assessment of one applicant. It was decided the review would not proceed for that individual until ASIO had concluded its reassessment. ASIO's reassessment was not concluded by the end of the reporting period.

During the 2012–13 reporting period the Independent Reviewer released her findings in relation to five applicants for review. In three cases, the Independent Reviewer formed the opinion the adverse security assessments issued by ASIO remain appropriate. In relation to two individuals, the Independent Reviewer formed the opinion the adverse security assessments are not appropriate and recommended ASIO issue either non-prejudicial or qualified security assessments. ASIO undertook new assessments of these two cases, resulting in the Director-General accepting the Independent Reviewer's recommendations and issuing non-prejudicial security assessments in relation to both individuals.

In addition, during the reporting period the Independent Reviewer referred 'new information' she received in the course of her review to ASIO in respect of two applicants. In accordance with the Terms of Reference, their reviews were temporarily suspended pending ASIO's consideration of the new information. At the end of the reporting period, ASIO's consideration of this information was ongoing.

No periodic reviews were undertaken during the reporting period as 12 months had not passed since the release of the Independent Reviewer's initial findings.

## Independent National Security Legislation Monitor

---

The Office of the Independent National Security Legislation Monitor (INSLM) was established by the *Independent National Security Legislation Monitor Act 2010*.

Mr Bret Walker SC was appointed as inaugural INSLM on 21 April 2011 to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation and to report to the Prime Minister and the parliament on an ongoing basis.

On 14 May 2013 the INSLM tabled his second annual report in parliament, the first report in which the INSLM made recommendations on national security legislation.

During 2012–13 the INSLM undertook an inquiry into the operation and effectiveness of terrorism financing legislation. At the time of publication, the INSLM's report in relation to this matter was still pending.

The INSLM also commenced an inquiry into the *National Security Information (Criminal and Civil Proceedings) Act 2004* during the reporting period. As at 30 June 2013 ASIO was finalising an initial submission to this inquiry.



## Legal assurance and capability protection

---

ASIO's Office of Legal Counsel (the office) assists ASIO manage its legal risk in carrying out its overt and covert activities, including through the provision of advice on the scope of ASIO's powers and functions and in relation to capability risks.

The office contributed to the implementation of ASIO's special powers operations by advising on whether the information available satisfies the legislative requirements; assessing and processing warrant documentation; overseeing the ongoing management of warrants in relation to timeliness; and providing of revocation and reporting documentation to the Attorney-General.

The office assisted ASIO in its response to external oversight and accountability mechanisms. This included the legislative reviews conducted by the INSLM and the work of the Independent Reviewer. In relation to advisory opinions of the Independent Reviewer, the office provided security intelligence advice to facilitate the open release of relevant information where possible, while protecting ASIO's intelligence capabilities where necessary.

The office provided a range of capability protection advice to support the merits review process in the AAT, and judicial review in the Federal Court and High Court of Australia.

The office also supported operational areas in the provision of security advice to inform Commonwealth agency decision-making. The office worked closely with ASIO's operational areas during the course of several security investigations. This included the provision of legal advice to support security assessment interview preparation, the legal evaluation of the intelligence case and the preparation of security assessment decision-making records. Notable resources were also directed to operational training. The office played an active role in training forums to promote legal considerations during the security assessment process and informed the development of policies and procedures.

The office provided legal and capability protection advice to support Organisational policy development and operations and to inform engagement with partner agencies. It also provided advice to inform the development of cross-governmental governance frameworks to enhance interoperability and developed workshops on evolving best practice.

## Legislative change

ASIO's Office of Legal Counsel works to ensure legislation affecting ASIO adequately equips and assists the Organisation to fulfil its functions, including by advocating for legislative amendment within a whole-of-government agenda.

### Public Interest Disclosure Act

The *Public Interest Disclosure Act 2013* (PID Act) received royal assent on 15 July 2013, outside the reporting period. The PID Act provides agencies and whistleblowers with procedures to follow in making a 'public interest disclosure', and protections for those who do so in accordance with the scheme.

During the reporting period ASIO undertook a large amount of work in reviewing draft legislation, briefing other departments on the practical application of proposed provisions in an intelligence context and advising relevant ministers and departments of potential issues associated with the enactment of particular provisions.

The process of consultation began in 2009 and culminated in final negotiations shortly before the introduction of the Public Interest Disclosure Bill on 21 March 2013. ASIO provided guidance in the development of the scheme, and more targeted legal scrutiny of the Bill and operative provisions occurred throughout the reporting period.

In ASIO's view, the resulting PID Act achieves a balance between ensuring the accountability of all agencies while still ensuring the ability of Australian Intelligence Community agencies to carry out their national security functions.

## Other reviews

---

### Council of Australian Governments review of counter-terrorism legislation

Following an intergovernmental agreement on counter-terrorism laws in 2004, new legislation was enacted throughout Australia to provide law enforcement with enhanced powers in dealing with terrorism and related matters. COAG agreed it was appropriate for these laws to be formally reviewed after five years.

On 6 August 2012 COAG commenced its review of the operation, effectiveness and implications of key counter-terrorism laws. ASIO provided a range of support to this significant review, including the provision of briefings to the COAG review committee, attendance at hearings, and a public submission setting out ASIO's views on key issues.

The COAG review committee tabled its report on 14 May 2013. This report contains 47 recommendations, which are currently being considered by government.

# Internal audits and fraud control

---

## Fraud control

The *Financial Management and Accountability Act 1997* requires ASIO to undertake a fraud risk assessment and implement a fraud control plan. In the reporting period ASIO underwent an organisational restructure, and new divisions and branches were established. ASIO fraud risks assumed new owners as responsibilities realigned, and this was seen as an ideal opportunity to refresh ASIO's fraud risk assessment.

This assessment identified a series of fraud risks that were found to be appropriately mitigated by controls in the ASIO security and financial frameworks. In June 2013 ASIO also implemented the *ASIO Fraud Control Plan 2013–15*, which outlines the Organisation's strategies to control and manage fraud.

During the reporting period ASIO received four allegations of fraud. Of these, three allegations were investigated and no fraud activities were identified. One allegation of fraud remains under investigation at the time of publishing. No external allegations of fraud were reported.

Fraud awareness training for all new employees and contractors continues to be a feature of ASIO induction training. ASIO also provides computer-based training modules on fraud awareness which ASIO officers are required to complete every three years.

ASIO is committed to the continual enhancement of its fraud control and management arrangements to ensure they reflect best practice. During the development of the ASIO Fraud Control Plan 2013–15, a fraud control and management workshop involving key internal stakeholders assessed existing fraud control and management arrangements and identified areas for improvement.

ASIO is vigilant in preventing, detecting and investigating fraud and will implement the outcomes of the ASIO fraud control and management workshop in a strengthening of ASIO's fraud control and management framework.

## Audit

In the reporting period, the Audit and Risk Committee sought to consolidate changes arising from its transition from the Audit and Evaluation Committee. These changes were in response to amendments to the Financial Management and Accountability Regulations to foster and entrench a positive risk culture. The independent chair of the committee has been in place for over 12 months and has guided the committee in embedding change and identifying opportunities for continuous improvement. The committee continues to fulfil its role of providing independent assurance and advice to the Director-General and the executive on a range of governance and compliance matters.

The focus of ASIO's internal audit program is to improve Organisational performance. This is achieved through the provision of a value-adding service to ASIO business areas, identifying potential business improvements and validating compliance with relevant legislation and established practices and processes.

One major review completed in 2012–13 assessed ASIO's compliance with the requirements of the *Work Health and Safety Act 2011* (WHS Act). This audit identified that ASIO is largely compliant with the mandatory requirements of the WHS Act and is undertaking a range of activities to establish or maintain conformance and to apply better practice.

ASIO has continued to undertake compliance audits to ensure the Organisation is conforming to privacy requirements and adhering to agreements made with external partners.

The Internal Audit team completed professional training to ensure the maintenance and development of their professional qualifications and to maintain awareness of contemporary audit and risk issues.

ASIO completed fieldwork with regard to operational expenditure across the Organisation to assist the Australian National Audit Office in conducting its financial statements audit. No issues requiring rectification were identified.

## Audit of assumed identities

Assumed identities and commercial cover are used to protect ASIO officers' identities and prevent the potential compromise of ASIO operational activities. Part IAC of the *Commonwealth Crimes Act 1914* establishes a Commonwealth scheme for the acquisition and use of assumed identities by members of intelligence and law enforcement agencies. As a participating agency, ASIO is required to maintain appropriate records about the operation of this scheme. These records are required to be audited at least once every six months, with a report provided to the IGIS.

Additionally, a small number of authorities are maintained under the *New South Wales Law Enforcement and National Security (Assumed Identities) Act 2010*; these are also audited six-monthly while active. ASIO audited its assumed identities during the reporting period. In respect of the legislation, a report will be sent to the NSW Minister for Police and Emergency Services as required by the NSW assumed identity legislation. This report will be accompanied by an audit declaration. Audits undertaken in respect of assumed identities did not identify any fraud or unlawful activity.



## Security in ASIO

---

ASIO requires a high level of protection around information and advice in order to fulfil its role. ASIO regards its security standard in this respect as best practice. To ensure ASIO achieves this standard, the Organisation continually develops and reviews both security policy and procedures. This policy foundation operates alongside an active security culture, contributed to by all officers, working to protect officers, premises and information from compromise.

### Security policy and coordination

In meeting requirements for the implementation of the PSPF, ASIO has reviewed and, where necessary, revised its internal security policies and procedures. ASIO also meets the PSPF's security governance requirements for the management and oversight of the Organisation's protective security.

### Personnel security

All ASIO officers hold high-level security clearances. To do so, they must meet whole-of-government security clearance requirements. This means they must be honest, trustworthy, mature, tolerant and loyal, and not susceptible to influence or coercion. Suitability to hold a clearance is established at entry and then continually assessed through a variety of Australian government-mandated and ASIO-specific checks and reviews.

## Information technology security

ASIO continues to implement tailored information security programs designed to protect ASIO's information and communications systems. These programs facilitate the review of system security compliance along with an audit capability to ensure system usage is authorised, appropriate and secure. Integral to the success of these programs is ASIO's commitment to uphold and foster a strong security culture which protects sensitive information—both national and personal—while facilitating appropriate and effective information sharing.

ASIO remains responsive to the changing IT environment adapting to global trends and challenges.

## Outreach

---

ASIO is committed to engaging effectively with a range of partners, including government departments, private industry and business, academia and the broader community. ASIO considers this aspect of its work critical to maintaining the security of Australia, its people and its interests.

Where possible, ASIO makes public comment and engages with the media and other interested parties. ASIO believes this is essential to maintaining public confidence in the work conducted by ASIO. However, ASIO adheres to the longstanding government policy of not commenting on specific intelligence matters. While providing more detailed public comment on matters would often reduce unfounded speculation and commentary on ASIO's work, deviation from this policy risks exposing ASIO's intelligence sources and methodologies and could compromise ASIO's ability to carry out its functions.

Some of the mechanisms through which ASIO communicates with the public include speeches and appearances by the Director-General, ASIO-initiated partnership forums for government and industry participants, the ASIO website and documents such as this unclassified ASIO report to parliament.

## ASIO Partnership Forum

ASIO Partnership Forums provide information sessions for senior officers from the national security community and broader government partners. These sessions are specifically tailored for individuals who work with ASIO on a regular or semi-regular basis and who need to develop a stronger appreciation of ASIO's roles and functions. The Partnership Forums aim to inform government agencies of ASIO's capabilities and the policy framework in which the Organisation operates. Participants are encouraged to share their agency priorities to help foster a better understanding of the broader security environment and the role of individual agencies within that environment.

## Business Liaison Unit

The BLU provides a public interface between the Australian Intelligence Community and Australian business in order to raise awareness of national security issues. The BLU administers a secure website containing intelligence-derived unclassified reporting on the domestic and international security environment, as well as physical, personnel and information security advice. The BLU engages directly with businesses on a one-on-one basis to help build strong relationships between ASIO and the private sector. This engagement seeks to enable Australian business security managers to recognise and respond to national security related threats, develop and implement appropriate risk management strategies, and provide informed briefings to executives and staff.

For further information, including contact details, visit the BLU website ([www.blu.asio.gov.au](http://www.blu.asio.gov.au)).

## Stakeholder Satisfaction Survey

The annual Stakeholder Satisfaction Survey provides ASIO with valuable insight into the level of satisfaction of key partners and the extent to which ASIO supports the attainment of partner agency outcomes. The survey also seeks feedback on partners' engagement with ASIO; their views on ASIO's collaboration, stakeholder focus, capabilities and people; and their evaluation of the quality, timeliness and accessibility of ASIO's information and advice.

During the reporting period, 38 representatives from 20 agencies were interviewed by a consultant. Interviews were extended this year to include Senior Executive Service Band 1 and 2, as well as heads of agency. Additional participants across all areas of the Commonwealth and state and territory governments were invited to provide feedback via the email component of the survey.

The majority of agencies interviewed noted an improvement in their engagement with ASIO. Ninety-seven per cent of interviewees rated their overall level of satisfaction with ASIO as 'highly satisfied' or 'mostly satisfied'.

A number of Australian government agencies noted ongoing improvement in ASIO's collaborative approach to achieving whole-of-government outcomes. Relationship-building activities including the ASIO Partnership Forums, at both the Senior Executive Service and middle-management levels, were also highlighted as key to this improvement.



## Public statements and media

The most efficient and effective way ASIO engages with the public is through the media, as well as speeches and appearances by the Director-General. This engagement seeks to address issues of public interest and raise awareness of important and contemporary security issues. Throughout the reporting period ASIO made public comments on a variety of topics, including the insider threat to government, the balance between individual freedoms and national security, the risks in a connected economy, and the changing security landscape.

Transcripts of public speeches by the Director-General are available on the ASIO website ([www.asio.gov.au](http://www.asio.gov.au)).

## Official history of ASIO

Work continued on the official history of ASIO by the ANU, under the direction of Professor David Horner AM. The official history will provide an independent account and assessment of ASIO's history from 1949 to 1989, giving unique insight into aspects of Australia's postwar social and political history, in particular the role of ASIO in significant national and international events.

Research has been undertaken in ASIO and the National Archives of Australia (NAA), and to date 4330 un-redacted ASIO files have been passed to the ANU team. Professor Horner has submitted a draft of the first volume of the history, covering 1949–63. ASIO has begun clearing the manuscript to ensure no information which might be prejudicial to national security is published. The first volume explains why ASIO was formed in 1949, describes ASIO's role in the defection of the Petrovs in 1954 and ends with the expulsion of Ivan Skripov in 1963. A process is underway to select a publisher for the history. Volume 1 will be published in 2014, with the final publishing date to be agreed with the publisher.

The History of ASIO Advisory Committee comprises two external representatives—Mr Geoff Gallop AC and Mr Jim Carlton AO—the Director-General and a Deputy Director-General. The committee meets every six months to monitor progress of the project and to ensure proper procedure, accountability and due process.

The second volume, covering 1963–89, is due for completion in 2015.





# Part 5

## CORPORATE MANAGEMENT

‘It is important that Australia maintains the best possible capability to protect both our national secrets and our critical infrastructure against those who might do us harm, or who seek to influence governments to act in ways that could distort our democratic processes or damage our national interests.’

► *Speech by the Director-General to the Australian Industry Group  
Annual National Forum  
20 August 2012*

# Corporate strategy and governance

## ASIO Strategic Plan 2013–16

ASIO has implemented a new strategic plan for the period 2013–16. This builds on the significant achievements and initiatives completed under the *ASIO Strategic Plan 2011–13*, including:

- ▶ delivery of an enhanced electronic document and record management system which has improved information capture, information sharing, collaboration and accountability;
- ▶ development and rollout of a new case management system, delivering significant efficiencies for staff, better recording of key decisions, enhanced accountability and more detailed reporting across ASIO's investigative caseload; and
- ▶ establishment of a new corporate committee structure, which ensures ASIO is better able to set strategic direction and effectively manage Organisational priorities and resources.

The *ASIO Strategic Plan 2013–16* will further assist the Organisation to focus on its critical priorities (see page 51) while responding with agility and resilience to emerging challenges.

## ASIO's governance committees

ASIO's governance committees provide strategic advice to the Director-General on the Organisation's corporate and operational activities. The ASIO Corporate Committee Framework places particular emphasis on the role of communication and leadership within ASIO.

### ASIO Executive Board

The ASIO Executive Board is the primary advisory committee supporting the Director-General in the governance of the Organisation. Its monthly meetings set ASIO's strategic direction and manage Organisational resources. The Executive Board is attended by the Director-General, the Deputy Directors-General and an external member.

### Supporting committees

The ASIO Executive Board is supported by a range of committees, each focusing on a separate aspect of ASIO's corporate or operational work. These committees provide advice which informs the Director-General's decision-making.

#### Intelligence Coordination Committee

The Intelligence Coordination Committee provides strategic direction for ASIO's operational activities, allocates resources according to investigative and assessment priorities and regularly reviews performance against benchmarks.

#### Workforce Capability Committee

The Workforce Capability Committee advises the ASIO Executive Board on matters relevant to maintaining the capacity and capability of ASIO's workforce necessary for the Organisation to meet its current and future needs.

<b>Mission</b>	To identify and investigate threats to security and provide advice to protect Australia, its people and its interests
<b>Vision</b>	The intelligence edge for a secure Australia

<b>Goals</b>	<b>Deliver high-quality security intelligence collection, analysis, assessment and advice in support of our mission</b>
	We excel in our use of security intelligence in support of our mission.
	We work with partners to ensure capabilities are managed to optimise security outcomes.
	We provide timely and accurate security intelligence advice to support decision-makers.
	We manage risk in a constantly evolving security environment.
	<b>Continue to enhance our strategic impact and reputation</b>
	We work effectively and collaboratively with national and international partners and are seen as a responsive and collegial partner.
	We are influential in shaping Australia's response to the national and international security environment.
	We promote security awareness and understanding across government and private industry.
	We provide leadership and expertise on security intelligence in support of our mission.
	<b>Evaluate, evolve and strengthen our capabilities and business practices</b>
	We are professional, with the flexibility, initiative and determination to anticipate and drive change.
We harness opportunities and address challenges presented by technology.	
We build accountability and evaluation into everything we do.	
We evaluate activities to strengthen future planning and decision-making.	
<b>Attract, develop and retain a professional and highly competent workforce</b>	
We exemplify excellence in security practices, cooperation, accountability and integrity.	
We develop and support people to succeed.	
We have a motivated, high-performing workforce who exemplify professionalism in all they do.	
We have a strong, unified leadership team who encourage and motivate others to achieve.	

### *Work Health and Safety Committee*

The Work Health and Safety (WHS) Committee builds cooperation between management and staff in formulating, implementing and reviewing health and safety policies, procedures and initiatives. It works to promote an anticipatory and proactive approach to WHS and foster a positive WHS culture.

### **Counter Intelligence and Security Review Committee**

The Counter Intelligence and Security Review Committee provides guidance and direction in respect of security policy for ASIO and sets counter-intelligence and security priorities. It also approves security policy and procedure documentation, and reviews the compliance of ASIO in meeting legislative and policy responsibilities specific to Australian government mandatory standards.

### *ASIO Security Committee*

The ASIO Security Committee reviews and addresses ASIO's security culture, framework and processes and ensures security risk management best practice is applied to ASIO people, property and information technology systems. It is also responsible for the development and integration of the government and ASIO's security policies and ensures Organisational accordance with legislative and policy responsibilities regarding protective security.

### **Finance Committee**

ASIO's Finance Committee provides advice and makes recommendations to the ASIO Executive Board on resource allocation, and financial management and strategy.

### *New Building Committee*

The New Building Committee provides strategic guidance on the progress of the New Building project, ensuring the building will meet ASIO's needs. The committee is also responsible for preparing and implementing a smooth and secure transition to the new building.

### **Audit and Risk Committee**

The Audit and Risk Committee provides independent advice to the Director-General on ASIO's risk, fraud control and compliance framework and its financial statement responsibilities. To ensure the committee is able to conduct its activities effectively, it is provided with wide authority to access information relevant to its role and responsibilities. The committee has an independent chair appointed by the Director-General.

## **Communication and leadership meetings**

### **Senior Executive Meeting**

The Senior Executive Meeting is a weekly meeting attended by officers at the Senior Executive Service Level 2 and above to discuss emerging corporate and operational issues. It is chaired by the Director-General.

### **Senior Executive Service Meeting**

The monthly Senior Executive Service Meeting provides a forum for officers at the Senior Executive Service Level 1 and above to discuss key strategic issues affecting ASIO.

## ASIO Consultative Council

The ASIO Consultative Council was established to enable management and staff of the Organisation to meet regularly in a structured way to discuss and resolve issues of interest and concern.

## Risk management

ASIO's commitment to risk management is outlined in the Strategic Risk Management Framework. An internal review of the framework was commenced in May 2013 to consider whether the framework continues to serve ASIO's needs or whether alternative models might yield enhanced outcomes.

This review was commenced in anticipation of the passage of the *Public Governance, Performance and Accountability Act 2013* (the PGPA Act), which came into effect on 1 July 2013.

While the PGPA Act is principally focused on finance law and the protection of public revenue, section 16 of the PGPA Act more generally requires the 'accountable authority of a Commonwealth entity' (in ASIO's case, the Director-General) to establish and maintain:

- ▶ an appropriate system of risk oversight and management for the entity; and
- ▶ an appropriate system of internal control for the entity.

The review is a collaborative effort by relevant internal stakeholders and is being developed for consideration by the ASIO Audit and Risk Committee and endorsement by the ASIO Executive Board.

The review of the framework was ongoing at the conclusion of the reporting period.

## ASIO internal performance reporting

ASIO conducts quarterly internal performance reporting, which is designed to capture cross-Organisational input regarding ASIO's performance against benchmarks. All divisions contribute to the evaluation of performance and to the refining of benchmarks to ensure relevance against Organisational activities.

## Enterprise resilience

ASIO has developed a range of plans to ensure continuity of services should a planned or unplanned event occur which disrupts regular business activities. These plans cover emergency management, business continuity and recovery, and integrated security requirements. The plans are scalable depending on the nature and size of the disruption.

The focus of enterprise resilience activities in 2012–13 was on preparing the Organisation to move from its current accommodation in Canberra to a new central office, in a minimally disruptive way.

# People

---

Throughout the 2012–13 reporting period, ASIO delivered a range of strategic programs to build long-term sustainability, following the realisation of the Organisation's period of significant growth. ASIO needs to be able to deliver security intelligence in an environment of complex security and fiscal challenges. Investments continue to be prioritised carefully to develop and sustain ASIO's ability to deliver critical capabilities now and into the future, to contribute to a safe and secure Australia.

## Human Capital Framework

The ASIO Human Capital Framework guides ASIO's approach to delivering people management outcomes. It is centred on the following key and interconnected elements:

- ▶ **people strategy and workforce planning**—supporting executive decision-making, strategic workforce planning and the management of sourcing and retention strategies;
- ▶ **selection, evaluation and vetting**—attracting and selecting talent and the core recruitment processes;
- ▶ **capability management, learning and development**—managing the performance of the workforce and ensuring continuous professional development; and
- ▶ **agility management, human resource services and support**—human resource policies and practices that create and manage agility in the workforce.

## People strategy and workforce planning

As at 30 June 2013 ASIO employed 1791.8 full-time equivalent staff.

During the reporting period ASIO's separation rate was 5.2 per cent, up from 4.7 per cent in 2011–12.

The ASIO Strategic Workforce Plan 2013–2016 was launched to supersede its 2011–2015 plan. The revised plan takes into account the impact of budgetary constraint and also acknowledges a change in focus from a period of organisational growth, to a new paradigm of stability and long-term people capability.

Workforce planning activity in 2012–13 included the development of specific plans for two priority areas: Visa Security Assessments and Travel Intelligence Branch; and Technical Capabilities Division. Detailed workforce plans were developed to enable ASIO to identify, manage and mitigate specific workforce risks and ensure it has the workforce capacity and capability to respond to current and future priorities.

In 2012–13 ASIO initiated a staffing and resource allocation review. This work provided the necessary framework to assist the Organisation to prioritise and realign staffing allocations and to ensure ASIO's capability to meet its ongoing obligations to government. With careful consideration of the retention and allocation of knowledge and skills, the review informed important workforce strategies, including an organisational restructure and a 25 per cent reduction in the numbers of ASIO's Senior Executive Service. The strategies arising from the staffing and resource allocation review, along with the Human Capital Framework, continue to inform workforce planning activities and ASIO's investment in skilling its personnel in order to enhance this nationally important security intelligence capability.

### **Career and Talent Management Framework**

In 2012–13 ASIO developed its Career and Talent Management Framework. Designed to address ASIO's capability needs for future roles and guide the career aspirations of employees, the framework acknowledges and reinforces a partnership between the individual and the Organisation, recognising that staff are individually accountable and active in managing their own careers, within a framework that provides guidance and development opportunities.

The framework aims to ensure ASIO has the capabilities required to deliver its mission and objectives by having 'the right person, in the right role, at the right time', and to provide opportunities for individuals to have satisfying careers in ASIO by:

- ▶ aligning the Organisation's needs and employees' needs in respect of development for future roles;
- ▶ encouraging employees to be accountable for acting on their career directions and aspirations;
- ▶ ensuring information and support resources about career and development opportunities, career paths and individual capabilities are readily available;
- ▶ providing clear guidance from senior managers in regard to opportunities, capabilities and development needs; and
- ▶ providing development opportunities that contribute to retaining and developing capability for individuals and the Organisation (including training programs, tertiary study, secondments, exchange programs, higher duties and staff mobility).

The Career and Talent Management Framework is underpinned by the ASIO Job Family Model, which was implemented in 2012–13 and allows the Organisation to identify and deliver more targeted recruitment and development strategies.

ASIO remained committed to its outreach with regard to secondments, with placements to and/or from the following government agencies:

- ▶ the Attorney-General's Department;
- ▶ the Australian Federal Police;
- ▶ the Australian Secret Intelligence Service;
- ▶ the Australian Geospatial-Intelligence Organisation (also known as the Defence Imagery and Geospatial Organisation);
- ▶ the Australian Signals Directorate (also known as the Defence Signals Directorate);
- ▶ the Defence Intelligence Organisation;
- ▶ the Department of Foreign Affairs and Trade;
- ▶ the Department of Immigration and Citizenship;
- ▶ the Office of Transport Security, within the Department of Infrastructure and Transport;
- ▶ the Office of National Assessments;
- ▶ the Department of the Prime Minister and Cabinet;
- ▶ the Department of Human Services;
- ▶ the Department of the Treasury;
- ▶ the New South Wales Police Force;
- ▶ the Queensland Police Service;
- ▶ Victoria Police; and
- ▶ Western Australia Police.

ASIO also participated in a number of exchanges with foreign partner agencies.

## Technical capability

As a result of the increasing importance of technical capability in intelligence operations, combined with the increased competition in the marketplace for technical skills, building ASIO's technical workforce requires priority attention. During the reporting period, a number of trainees were recruited for the ASIO IT traineeship, a key strategy for building ASIO's information and communications technology workforce. A Technical Capabilities Workforce Plan was developed to identify and manage the specific challenges of attracting and retaining quality technical staff. The recruitment and development strategies that resulted from this plan will continue to shape ASIO's activities throughout 2013–14.

## Selection, evaluation and vetting

Maintaining and developing ASIO's capability through a highly effective cadre of intelligence professionals remains a key priority for ASIO. Given the significant lead time to recruit, train and develop this capability, recruitment of intelligence professionals will continue on a regular basis into the future.

ASIO's recruitment activities in 2012–13 focused on intelligence professionals, technical officers and security assessors. ASIO strengthened its 'grow your own' strategies to attract and develop entry-level staff and existing staff within a range of professional disciplines, expertise and backgrounds. An essential element of refinement in ASIO's recruitment and marketing strategy was the increased use of specialist online media to promote employment opportunities in niche areas of the Organisation.



ASIO's expenditure on recruitment advertising decreased from \$398 592 in 2011–12 to \$317 729 in 2012–13.

## Capability management, learning and development

### Staff mobility

In 2012–13 ASIO launched its Organisational Capability Program, which underpins the development of the human capability and capacity required by ASIO to ensure delivery against its mission. The first phase of the program concentrates on intelligence roles.

The program consists of structured job placements and associated experiences for staff across all locations to:

- ▶ enhance ASIO's individual and whole-of-Organisation skills, experience and knowledge;
- ▶ develop skills and capabilities across a greater number of staff so ASIO is better placed to respond to rapidly emerging priorities and issues;
- ▶ meet the Organisation's requirement for breadth and depth of experience; and
- ▶ provide flexibility for officers to balance their careers with personal and family responsibilities.

### Study and language development programs

ASIO's capability requirements continue to evolve in response to changes in the operating environment. Accordingly, training and professional development continue to be important investments in building and sustaining intelligence and security capability.

ASIO supports training and professional development for officers through internal and external opportunities. This includes external programs provided by the Australian Public Service Commission; the National Security College, at the Australian National University (ANU); the National Intelligence Community Training Secretariat; and private sector providers.

Support for external study opportunities continued throughout the year, with officers accessing ASIO's study assistance and language skills development programs. Both programs are aimed at encouraging officers to undertake professional development in areas relevant to their roles in ASIO and broader government.

Over the past year 145 officers participated in ASIO's Study Support Program in fields of study including business management, policy, project management and information technology. ASIO's Language Skills Development Program provided support to 26 officers across a range of languages. Both programs offer fully funded or partially funded support.

## Management and leadership development

In 2012–13 ASIO's leadership program, Leading Edge, concluded. The program built a common and practical understanding of the Organisation's strategic priorities across ASIO's whole leadership group, and all of the Organisation's senior leaders attended it during 2010–12. Over the three years the program was run, over 95 per cent of participants reported it would enhance the way they worked and was a valuable investment.

In early 2013 a new Management and Leadership in Security Intelligence strategy was developed. The strategy will focus on building and reinforcing fundamental management skills and knowledge, and help managers to deliver strong workplace leadership, all underpinned by effective management practice.

The strategy places emphasis on developing management and leadership skills, operational and investigative excellence and intellectual rigour and providing timely advice to government. In positioning ASIO for the future, the strategy will enable:

- ▶ managers and leaders to continue to be ahead of a rapidly changing security environment to meet the expectations of government and the public;
- ▶ succession planning to prepare and support leaders to achieve strategic goals;

- ▶ ASIO's management and leadership cohort to deal effectively with operational, investigative and workplace/workforce issues; and
- ▶ the continued sharing of knowledge and information, both internally and externally.

## Rewards and Recognition

ASIO recognises the achievement of teams and individuals across the Organisation. The Rewards and Recognition policy focuses on identifying outstanding achievement in a range of endeavours and provides a forum in which this is acknowledged more broadly by management and colleagues. It reinforces ASIO's Values and Code of Conduct and ASIO's commitment to excellence at all levels within the Organisation.

Officers' achievements are recognised both informally and formally throughout the year. Formal recognition ceremonies are held twice yearly and recognise ASIO officers' contributions in areas such as leadership, innovation, analytical and operational effectiveness, dedication to community-based work, and exceptional service.

Managers also incorporate working-level reward processes in their line areas throughout the year to recognise the contributions of officers as they occur.

## e-Learning

ASIO's e-learning system continues to deliver competency-based training for work health and safety, workplace behaviour, ethics and other mandatory training requirements. Three e-learning modules on reporting standards, and several modules for new and existing IT systems, were implemented to assist in achieving Organisational outcomes.

### CASE STUDY: SHARED E-LEARNING CAPABILITY

As part of ASIO's expanding collaboration with other investigative agencies, the Training and Development e-learning team designed and developed the e-learning course Internet for Investigators, on request from the National Interception Technical Assistance Centre (NiTAC). This course supports the NiTAC goal of helping law enforcement and investigatory agencies transition to internet-based investigations, by supplying suitable education programs. The program has been released to 16 agencies, including various law enforcement agencies across Australia. It is expected that ongoing collaboration will generate more training and development opportunities into the future.

## Intelligence training

ASIO's Intelligence Development Program (IDP) provides focused and flexible training for intelligence professionals. The IDP training remained a cornerstone of ASIO's intelligence training program and provided fundamental skills to officers in analytical and operational disciplines. Two IDPs were completed in the reporting period, with 35 intelligence professionals graduating and commencing their first posting.

An important feature of ASIO's intelligence training is the provision of specific training modules to officers who identify a need in order to perform aspects of their role. ASIO provided an additional 51 instances of analytical and operational training to these officers of between 5 days and 3 weeks duration.

ASIO's dedicated post-IDP training unit has continued to work in collaboration with the relevant divisions to deliver advanced and specialised courses, enhancing the skills of practising intelligence professionals. These additional courses have also reflected ASIO's own strategic shifts to ensure its cadre of intelligence professionals and leaders are meeting ASIO's organisational priorities.

## Agility management, human resources services and support

### Employment framework

In 2012 ASIO commenced a major review and consolidation of its employment framework, which comprises determinations, policies and guidelines. The review was undertaken to amalgamate existing determinations into a single reference point: the Consolidated Determination. The Consolidated Determination reflects the Organisation's contemporary approach to people management, aligns with public sector best practice and supports sound decision-making. In support of the Consolidated Determination, over 30 human resource policies and guidelines have been reviewed and endorsed by the ASIO Consultative Council. The Consolidated Determination and associated policies were released in September 2013 and will provide ASIO with a robust and transparent framework under which to commence negotiations for the 10<sup>th</sup> Workplace Agreement (2014–17).

### Professional Conduct and Behaviour Strategy

During the first quarter of 2013 ASIO commenced work on a comprehensive and updated strategy focusing on the professional conduct and behaviour of ASIO officers. The strategy encompasses awareness programs clearly communicating ASIO's expectations concerning workplace behaviour, as well as developing robust systems for identifying and responding to allegations of inappropriate behaviour and misconduct.

This strategy is being developed in recognition of recent changes to the *Fair Work Act 2009*, the introduction of the WHS Act and the impending finalisation of Safe Work Australia's draft Code of Practice: Preventing and Responding to Workplace Bullying. While reducing the likelihood of bullying occurring in the workplace is an important objective of the Professional Conduct and Behaviour Strategy, ASIO has chosen to take a more holistic approach and consider all forms of inappropriate workplace behaviour.

ASIO's Values and Code of Conduct form the foundation for how it operates as an Organisation. Accordingly, a critical element of the strategy will be a review of the Organisation's Values and Code of Conduct to ensure they continue to support and reinforce ASIO's commitment to the highest levels of professionalism and respect for others. This review will also give consideration to the recent amendments to the Australian Public Service Values, Code of Conduct and Employment Principles, introduced in July 2013 as part of amendments to the *Public Service Act 1999*.

### Ombudsman

The Organisation engages the services of an external Ombudsman to act as an independent arbiter in relation to staff issues or concerns, usually after internal mechanisms for resolution have been exhausted. The Ombudsman provides a biannual update to ASIO's Executive Board on the general nature of the matters raised.

In 2012–13 nine matters were formally referred by the Director-General to the Ombudsman:

- ▶ Seven matters were reviews of complaints (six completed and one commenced).
- ▶ Two matters were preliminary work on two separate projects:
  - ▷ reforms to ASIO's Values and Code of Conduct; and
  - ▷ a review of the scope of the Ombudsman role within the Organisation.

The Ombudsman responded informally to approximately 20 queries from officers.

### Work health and safety

In 2012–13 much of ASIO's focus in work health and safety (WHS) was the implementation and embedding of the WHS legislation that came into effect on 1 January 2012. Activities included:

- ▶ production of the ASIO Health and Safety Risk Management Framework;
- ▶ review and development of WHS policy;
- ▶ confirmation of 'officers', as defined under the WHS Act;
- ▶ education of those identified as having managerial responsibility under the WHS Act;
- ▶ review of the WHS Committee Terms of Reference;
- ▶ review of work groups; and
- ▶ the election and training of health and safety representatives.

An internal audit was carried out to determine ASIO's preparedness for and subsequent compliance with the WHS Act. The audit report has been shared with Comcare. The audit found the Organisation generally compliant against the criteria, with only minimal work required to improve compliance. Work has already been completed to update e-learning packages, update and develop WHS policies and develop key performance indicators.

In 2012 ASIO invited Comcare to conduct an audit of its rehabilitation management system to provide a benchmark of how effectively it is meeting its obligations under the *Safety, Rehabilitation and Compensation Act 1988*. Conformance was 70 per cent, with most areas of nonconformance relating to criteria 2 (Planning) and 4 (Measurement and Evaluation). In accordance with the requirements of the 2012 *Guidelines for rehabilitation authorities*, issued by Comcare, an annual audit program has been established.

During 2012–13 absences due to work-related injuries decreased by over 13 per cent compared to 2011–12, continuing a downward trend established in 2010–11.

Reporting period	Absence due to work-related injury (weeks)
2007–08	313.98
2008–09	362.03
2009–10	457.66
2010–11	380.80
2011–12	302.55
2012–13	260.83

ASIO has a strong focus on active case management to mitigate the risk, cost and personal impacts associated with long-term people management issues and to support line managers in resolving complex staffing situations.

In 2012–13 no notifications were made to Comcare and no investigations were conducted, nor were any notices issued to ASIO under the WHS Act.

To continue to promote the physical, mental and social health and wellbeing of its officers, ASIO held its annual health program in October 2012. The program activities were well attended by officers.

The Staff and Family Liaison Office is approaching its fourth year of operation and officers continue to access its services, particularly by those who are required to relocate interstate or overseas.

The regular family information nights continue to be well attended increasing understanding of the business of the Organisation for both officers and their families. In late 2012 ASIO introduced an engagement program with its regional offices aimed at communicating responsibilities under newly passed WHS legislation to a broader range of people at a local level.

## ASIO NOMINATION FOR A COMCARE AWARD

Comcare, the federal health and safety scheme manager, provides recognition and rewards to Commonwealth agencies demonstrating excellence in the rehabilitation and return to work of injured workers.

ASIO's nomination for an award was based on improvements in return-to-work outcomes since 2009, including the establishment of effective early intervention measures and a significant reduction in time off work.

From 2009 to 2012, despite a 27 per cent increase in the number of employees, the following improvements were achieved:

- ▶ 91 per cent reduction in incapacity weeks;
- ▶ 60 per cent reduction in frequency of lost time claims;
- ▶ 52 per cent reduction in likely future costs of claims;
- ▶ 42 per cent reductions in injuries resulting in incapacity; and
- ▶ 25 per cent reduction in premium rate for 2012–13.

The nomination went through a rigorous selection process by the Comcare Awards Panel to be assessed in the 'Rehabilitation and return to work' category, which recognises organisations that demonstrate excellence in this area. On 8 July 2013 Comcare announced ASIO as one of three finalists in this category.

# Property

---

## New central office

This project will provide a purpose-built facility, designed to cater for ASIO's technical and accommodation needs. With a minimum estimated design life of 50 years, the building is owned by the Department of Finance and Deregulation and leased to ASIO as the main tenant agency. Space in the new building has been allocated to accommodate the new Australian Cyber Security Centre.

Throughout 2012–13 construction of ASIO's new central office faced significant challenges, including the collapse of some key subcontractors. Construction is now substantially complete, with the remaining work effort concentrating on the commissioning of the complex building management and security systems.

The delays have contributed to continuing pressure on the project's budget, and cost overruns increased slightly in 2012–13 to \$44 million. This equates to an increase of 7.5 per cent over the approved budget of \$589 million. It is important to consider these budgetary pressures and scheduling delays in the context of the complexity and tenure of the project, given the budget and construction schedule were approved in 2008.

Throughout 2012–13 ASIO continued to undertake an Organisation-wide change management program in preparation for relocation to the new central office. Planning for the relocation is now generally complete.

## Estate and asset management

In anticipation of the move to ASIO's new central office building, a key focus has continued to be the effective management of current assets, including equipment and facilities. Due to the delay in moving to the new central office, ASIO has had to invest in further extending the life cycle of some current assets that will not be relocated.

## Environmental performance

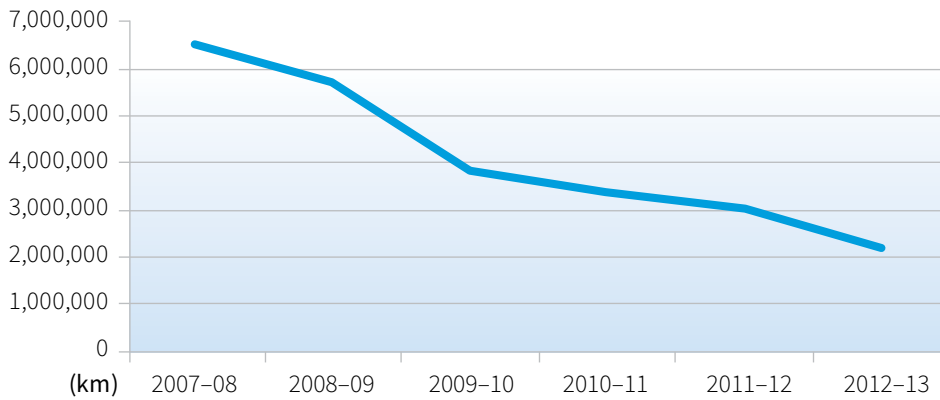
ASIO is committed to reducing its carbon footprint and implemented green initiatives during the reporting period to achieve this goal, including:

- ▶ a saving of 174 500 kilowatt hours, or 0.9 per cent of total electrical energy consumption, compared to the previous year;
- ▶ a 7.6 per cent reduction in natural gas energy consumption compared to the previous year;
- ▶ implementation of an environmental management system (EMS). The EMS will assist ASIO to meet environmental obligations and compliance with local government requirements, Australian standards and national legislation, as well as improve in ASIO's environmental performance and contribute to environmentally sustainable development;
- ▶ recycling of paper products, toner cartridges, scrap metal, fluorescent light tubes and batteries;

- ▶ installation of energy-efficient lighting and refinements to operating times for building lighting and air conditioning; and
- ▶ a reduction in the distance travelled by corporate passenger vehicles by a total of 832 728 kilometres (see Figure 1).

ASIO participated in the sixth consecutive Earth Hour event on 23 March 2013.

Figure 1: ASIO Senior Executive Service and pool vehicles—total distance travelled (kilometres)





# Financial services

---

## Purchasing

Throughout 2012–13 ASIO continued to adhere to the Commonwealth Procurement Rules and associated policy and guidelines. This involved exercising contemporary procurement advice and methodology in order to ensure ASIO's procurement activities are effectively managed and deliver value for money.

Details of ASIO's agreements, contracts and standing offers are confidential and not included in the unclassified ASIO report to parliament. These are available to members of the Parliamentary Joint Committee on Intelligence and Security, who have oversight of ASIO's administration and expenditure.

ASIO does not manage any expenditure types that require reporting under the Australian government Spatial Reporting Framework.

## Consultants

ASIO entered into 20 new consultancy contracts during 2012–13, resulting in total actual expenditure of \$835 878. In addition, five ongoing consultancy contracts were active during the reporting period, involving total actual expenditure of \$462 501. Total consultancy expenditure has decreased by \$747 279 from 2011–12.

Subject to authorised exemption for the protection of national security, a list of consultancy contracts let to the value of \$10 000 or more, inclusive of GST, and the total value of each of those contracts over the life of each contract may be made available to members of parliament as a confidential briefing or to the PJCS on request.

## Competitive tendering and contracting

ASIO participated in 35 open tenders during 2012–13. Other approaches to market were not advertised publicly for reasons of national security, in accordance with clause 2.6 of the Commonwealth Procurement Rules.

## Legal services

ASIO's Office of Legal Counsel provides in-house advice and services in respect of ASIO's human resource functions and commercial legal services to inform procurement and contractual arrangements.

Significant resources were directed to support the Organisational review of staff terms and conditions and supporting policies, with the objective of ensuring ASIO's employment and people management frameworks meet all legislative requirements. This included advising on the legal framework for restructured terms and conditions of employment, drafting provisions to reflect existing and new terms and conditions, advising on the operation of relevant legislation, such as the *Fair Work Act 2009*, and providing advice to support the review of policies that underpin the terms and conditions.

# Information and technology services

## Release of ASIO records

ASIO is an exempt agency under the *Freedom of Information Act 1982* (FOI Act) but is required to release its records under the *Archives Act 1983*. Amendments to the FOI Act and subsequently the Archives Act in May 2010 reduced the 'closed' period for access from 30 years to 20 years. This change was implemented in 1 January 2011 with a transition period whereby two years of records become available each year for the next 10 years, with full implementation by 2020.

It is ASIO's responsibility to ensure public access is managed in accordance with the requirement to protect sensitive national security information. Requests for access to ASIO records that are in the 'open' period are made to the NAA. The application is then sent to ASIO; the applicant remains anonymous. ASIO locates and assesses any relevant records and then provides advice to the NAA about whether the records contain information that should be exempt from public release under section 33(1) of the Archives Act.

Information is considered for exemption only on the basis of whether its release would damage national security now, not whether it was sensitive 20–30 years ago. In most cases, the information is released. Once a record is assessed and released to the NAA, it is available for access by any person or group.

Any member of the public can request to access an ASIO record. Family members are usually interested in obtaining their own records or finding out about their family history. Sometimes people who have been members of a group that may have been of investigative interest to ASIO will request records of that group. Researchers and writers use ASIO records as a useful resource. There are no limits to the number of requests a researcher or applicant can submit. To help manage the demand for access to ASIO records, NAA asks researchers or applicants with multiple requests for records identify a priority list. ASIO then processes these requests in priority order. With the agreement of the PJCIS and the IGIS, ASIO gives priority to requests from people seeking records on themselves or family members.

During 2012–13 there was a decrease in the number of applications made for access to records. A total of 357 requests were completed in 2012–13.

	2011–12	2012–13
Applications for record access	631	441
Requests completed	505	357
Number of pages examined	68 608	44 141

Applicants dissatisfied with exemptions by ASIO may request reconsideration of the decision by the NAA. In 2012–13, one internal reconsideration was processed and the NAA upheld the ASIO decision. Applicants may also appeal exemptions to the AAT and also appeal if their application is not completed within 90 days. One applicant has commenced AAT action against the Deemed Refusal of Access to a large number of records. This action involves records from ASIO and other government agencies. ASIO is liaising with NAA on this matter.

Applicants may lodge a complaint with the IGIS if they have concerns about accessing ASIO records. In 2012–13 ASIO was subject to one IGIS preliminary inquiry regarding a request for access to ASIO records. ASIO provided a response to the IGIS, who decided not to proceed with a formal inquiry.

## Upgrading recordkeeping capabilities

In 2012–13 ASIO continued to improve and upgrade electronic document and records management system in accordance with the Australian Government Digital Transition Policy, managed by the NAA. These enhancements also provide increased efficiencies for ASIO's information management and recordkeeping.

## International connectivity

ASIO's efforts to maintain close communications with overseas partners recognise the global nature of security threats. International cooperation supports ASIO's role in the provision of quality advice to government.

## Information and communications technology engagement

As part of the national security community, ASIO works collaboratively with PMC to progress the National Security Information Environment Roadmap: 2020 Vision. ASIO's Chief Information Officer is a board member of several domestic and international forums and committees that focus on improving information sharing within and across intelligence communities.





# Part 6

## FINANCIAL STATEMENTS

'I think the national investment in counter-terrorism has definitely contributed to stronger protection for Australians, but our efforts and capabilities need to be sustained.'

► *Speech by the Director-General to the Security in Government Conference  
4 September 2012*



## STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2013 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.



**David Irvine**  
Director-General of Security

28 August 2013







## INDEPENDENT AUDITOR'S REPORT

### To the Attorney-General

I have audited the accompanying financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2013, which comprise: a Statement by the Director-General of Security; Statement of Comprehensive Income; Balance Sheet; Statement of Changes in Equity; Cash Flow Statement; Schedule of Commitments; Schedule of Contingencies; and Notes to and forming part of the Financial Statements comprising a Summary of Significant Accounting Policies and other explanatory information.

#### *Director-General of Security's Responsibility for the Financial Statements*

The Director-General of Security is responsible for the preparation of financial statements that give a true and fair view in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards, and for such internal control as is necessary to enable the preparation of the financial statements that give a true and fair view and are free from material misstatement, whether due to fraud or error.

#### *Auditor's Responsibility*

My responsibility is to express an opinion on the financial statements based on my audit. I have conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. These auditing standards require that I comply with relevant ethical requirements relating to audit engagements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the Australian Security Intelligence Organisation's preparation of the financial statements that give a true and fair view in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Australian Security Intelligence Organisation's internal control. An audit also includes evaluating the appropriateness of the accounting policies used and the reasonableness of accounting estimates made by the Director-General

of Security of the Australian Security Intelligence Organisation, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

***Independence***

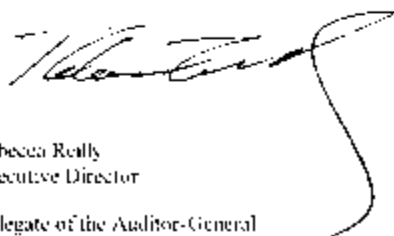
In conducting my audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

***Opinion***

In my opinion, the financial statements of the Australian Security Intelligence Organisation:

- (a) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards; and
- (b) give a true and fair view of the matters required by the Finance Minister's Orders including the Australian Security Intelligence Organisation's financial position as at 30 June 2013 and of its financial performance and cash flows for the year then ended.

Australian National Audit Office



Rebecca Reilly  
Executive Director

Delegate of the Auditor-General

Canberra

28 August 2013

## STATEMENT OF COMPREHENSIVE INCOME for the period ended 30 June 2013

	Notes	2013 \$ '000	2012 \$ '000
<b>EXPENSES</b>			
Employee benefits	3A	213,075	208,386
Suppliers	3B	132,843	146,299
Depreciation and amortisation	3C	56,421	40,173
Finance costs	3D	179	807
Write-down and impairment of assets	3E	11,058	434
Losses from asset sales	3F	161	137
Foreign exchange losses		(1)	2
<b>Total expenses</b>		<b>413,736</b>	<b>396,238</b>
<b>Less:</b>			
<b>OWN-SOURCE INCOME</b>			
<b>Own-source revenue</b>			
Sale of goods and rendering of services	4A	27,565	21,082
<b>Total own-source revenue</b>		<b>27,565</b>	<b>21,082</b>
<b>Gains</b>			
Rental income	4B	1,007	1,306
Other gains	4C	490	232
<b>Total gains</b>		<b>1,497</b>	<b>1,538</b>
<b>Total own-source income</b>		<b>29,062</b>	<b>22,620</b>
<b>Net cost of services</b>		<b>384,674</b>	<b>373,618</b>
Revenue from government	4D	329,743	328,124
<b>Deficit attributable to the Australian government</b>		<b>(54,931)</b>	<b>(45,494)</b>
<b>OTHER COMPREHENSIVE INCOME</b>			
Changes in asset revaluation surplus		9,828	-
<b>Total comprehensive loss attributable to the Australian government</b>		<b>(45,103)</b>	<b>(45,494)</b>

The above statement should be read in conjunction with the accompanying notes.

## BALANCE SHEET

### as at 30 June 2013

	Notes	2013 \$ '000	2012 \$ '000
<b>ASSETS</b>			
<b>Financial assets</b>			
Cash and cash equivalents		14,217	12,775
Trade and other receivables	5A	205,048	234,183
Other financial assets	5B	6,178	4,378
<b>Total financial assets</b>		<b>225,443</b>	<b>251,336</b>
<b>Non-financial assets</b>			
Land and buildings	6A,D	265,258	212,695
Property, plant and equipment	6B,D	78,744	78,779
Intangibles	6C,E	19,359	15,440
Other non-financial assets	6F	14,640	15,503
<b>Total non-financial assets</b>		<b>378,001</b>	<b>322,417</b>
<b>Total assets</b>		<b>603,444</b>	<b>573,753</b>
<b>LIABILITIES</b>			
<b>Payables</b>			
Suppliers	7A	14,026	14,785
Lease incentives	7B	2,201	2,756
Other payables	7C	20,314	9,297
<b>Total payables</b>		<b>36,541</b>	<b>26,838</b>
<b>Provisions</b>			
Employee provisions	8A	58,085	58,867
Restoration obligations	8B	10,024	9,979
<b>Total provisions</b>		<b>68,109</b>	<b>68,846</b>
<b>Total liabilities</b>		<b>104,650</b>	<b>95,684</b>
<b>Net assets</b>		<b>498,794</b>	<b>478,069</b>
<b>EQUITY</b>			
<b>Parent equity interest</b>			
Contributed equity		553,907	488,079
Reserves		17,930	8,102
Retained surplus (deficit)		(73,043)	(18,112)
<b>Total equity</b>		<b>498,794</b>	<b>478,069</b>

The above statement should be read in conjunction with the accompanying notes.

## STATEMENT OF CHANGES IN EQUITY for the period ended 30 June 2013

	Retained Earnings		Asset Revaluation Surplus		Contributed Equity/Capital		Total Equity	
	2013	2012	2013	2012	2013	2012	2013	2012
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>Opening Balance</b>	<b>(18,112)</b>	27,382	<b>8,102</b>	8,102	<b>488,079</b>	427,045	<b>478,069</b>	462,529
<b>Comprehensive Income</b>								
Other Comprehensive Income	-	-	<b>9,828</b>	-	-	-	<b>9,828</b>	-
(Deficit)/Surplus for the period	<b>(54,931)</b>	(45,494)	-	-	-	-	<b>(54,931)</b>	(45,494)
<b>Total comprehensive income</b>	<b>(54,931)</b>	(45,494)	<b>9,828</b>	-	-	-	<b>(45,103)</b>	(45,494)
<b>Transactions with Owners</b>								
<b>Contributions by Owners</b>								
Equity injection – appropriation	-	-	-	-	<b>5,062</b>	41,806	<b>5,062</b>	41,806
Departmental capital budget	-	-	-	-	<b>60,766</b>	19,228	<b>60,766</b>	19,228
<b>Total transactions with owners</b>	-	-	-	-	<b>65,828</b>	61,034	<b>65,828</b>	61,034
<b>Closing Balance attributable to the Australian government</b>	<b>(73,043)</b>	(18,112)	<b>17,930</b>	8,102	<b>553,907</b>	488,079	<b>498,794</b>	478,069

The above statement should be read in conjunction with the accompanying notes.

## CASH FLOW STATEMENT for the period ended 30 June 2013

	Notes	2013 \$ '000	2012 \$ '000
<b>OPERATING ACTIVITIES</b>			
<b>Cash received</b>			
Appropriations		394,815	427,493
Sales of goods and rendering of services		24,092	20,202
Net GST received		14,263	11,041
Other		3,893	12,463
<b>Total cash received</b>		<b>437,063</b>	<b>471,199</b>
<b>Cash used</b>			
Employees		213,455	195,772
Suppliers		153,587	168,935
Section 31 receipts transferred to OPA		29,297	19,856
<b>Total cash used</b>		<b>396,339</b>	<b>384,563</b>
<b>Net cash from operating activities</b>	9	<b>40,724</b>	<b>86,636</b>
<b>INVESTING ACTIVITIES</b>			
<b>Cash received</b>			
Proceeds from sales of property, plant and equipment		729	884
<b>Total cash received</b>		<b>729</b>	<b>884</b>
<b>Cash used</b>			
Purchase of property, plant and equipment		44,753	133,806
Purchase of intangibles		10,618	13,859
<b>Total cash used</b>		<b>55,371</b>	<b>147,665</b>
<b>Net cash used by investing activities</b>		<b>( 54,642)</b>	<b>( 146,781)</b>
<b>FINANCING ACTIVITIES</b>			
<b>Cash received</b>			
Contributed equity		15,360	54,034
<b>Total cash received</b>		<b>15,360</b>	<b>54,034</b>
<b>Net cash from financing activities</b>		<b>15,360</b>	<b>54,034</b>
<b>Net increase (decrease) in cash held</b>		<b>1,442</b>	<b>( 6,110)</b>
Cash and cash equivalents at the beginning of the reporting period		12,775	18,885
<b>Cash and cash equivalents at the end of the reporting period</b>		<b>14,217</b>	<b>12,775</b>

The above statement should be read in conjunction with the accompanying notes.

## SCHEDULE OF COMMITMENTS

### as at 30 June 2013

	Notes	2013 \$ '000	2012 \$ '000
<b>BY TYPE</b>			
<b>Commitments receivable</b>			
Sublease rental income		985	1,993
Net GST recoverable on commitments		62,550	11,962
<b>Total commitments receivable</b>		<b>63,535</b>	<b>13,955</b>
<b>Commitments payable</b>			
<b>Capital commitments</b>			
Land and buildings	A	-	36,716
Property, plant and equipment	A	3,574	15,885
Intangibles		842	275
<b>Total capital commitments</b>		<b>4,416</b>	<b>52,876</b>
<b>Other commitments</b>			
Operating leases	B	664,555	91,063
Other		23,649	29,713
<b>Total other commitments</b>		<b>688,204</b>	<b>120,776</b>
<b>Net commitments by type</b>		<b>629,085</b>	<b>159,697</b>

Commitments are GST inclusive where relevant.

No contingent rentals exist. There are no renewal or purchase options available to ASIO.

- A. Buildings, plant and equipment commitments are primarily contracts for purchases of fit-out, furniture and fittings for a new building.
- B. Operating leases included are effectively non-cancellable and comprise:
- *Agreements for the provision of motor vehicles to senior executive and other officers*
  - *Leases for office accommodation*
- Various arrangements apply to the review of lease payments:
- annual review based on upwards movement in the consumer price index (CPI);
  - biennial review based on the CPI; and
  - biennial review based on market appraisal.

## SCHEDULE OF COMMITMENTS

### continued

	2013	2012
Notes	\$ '000	\$ '000
<b>BY MATURITY</b>		
<b>Commitments receivable</b>		
<b>Operating lease</b>		
One year or less	985	976
From one to five years	–	1,017
<b>Total operating lease income</b>	<b>985</b>	<b>1,993</b>
<b>Other commitments receivable</b>		
One year or less	6,134	5,584
From one to five years	21,259	5,206
Over five years	35,157	1,172
<b>Total other commitments receivable</b>	<b>62,550</b>	<b>11,962</b>
<b>Total commitments receivable</b>	<b>63,535</b>	<b>13,955</b>
<b>Commitments payable</b>		
<b>Capital commitments</b>		
One year or less	4,416	52,876
From one to five years	–	–
<b>Total capital commitments</b>	<b>4,416</b>	<b>52,876</b>
<b>Operating lease commitments</b>		
One year or less	48,608	22,805
From one to five years	229,223	55,370
Over five years	386,724	12,888
<b>Total operating lease commitments</b>	<b>664,555</b>	<b>91,063</b>
<b>Other commitments</b>		
One year or less	17,254	26,058
From one to five years	6,395	3,655
<b>Total other commitments</b>	<b>23,649</b>	<b>29,713</b>
<b>Total commitments payable</b>	<b>692,620</b>	<b>173,652</b>
<b>Net commitments by maturity</b>	<b>629,085</b>	<b>159,697</b>

The above schedule should be read in conjunction with the accompanying notes.



## SCHEDULE OF CONTINGENCIES as at 30 June 2013

	2013	2012
	\$ '000	\$ '000
<b>Contingent liabilities</b>		
Claims for damages or costs	210	–
<b>Total contingent liabilities</b>	210	–
<b>Net contingent liabilities</b>	210	–

Details of each class of contingent liabilities and assets, including those not included above because they cannot be quantified or are considered remote, are disclosed in Note 10: Contingent Liabilities and Assets.

The above schedule should be read in conjunction with the accompanying notes.

## NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS for the year ended 30 June 2013

- Note 1: Summary of Significant Accounting Policies
- Note 2: Events after the Balance Sheet Date
- Note 3: Expenses
- Note 4: Income
- Note 5: Financial Assets
- Note 6: Non-Financial Assets
- Note 7: Payables
- Note 8: Provisions
- Note 9: Cash Flow Reconciliation
- Note 10: Contingent Liabilities and Assets
- Note 11: Remuneration of Auditors
- Note 12: Senior Executive Remuneration
- Note 13: Financial Instruments
- Note 14: Appropriations
- Note 15: Compensation and Debt Relief
- Note 16: Reporting of Outcomes
- Note 17: Net Cash Appropriation Arrangements

## Note 1: Summary of Significant Accounting Policies

### 1.1 Objective of ASIO

ASIO is an Australian government-controlled entity. It is a not-for-profit entity. The objective of ASIO is to provide advice, in accordance with the ASIO Act, to ministers and appropriate agencies and authorities, to protect Australia and its people from threats to national security.

ASIO is structured to meet the outcome: *To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government.*

ASIO activities contributing towards the outcome are classified as departmental. Departmental activities involve the use of assets, liabilities, revenues and expenses controlled or incurred by ASIO in its own right.

The continuing existence of ASIO in its present form and with its present programs is dependent on government policy and on continuing appropriations by Parliament.

### 1.2 Basis of Preparation of the Financial Statements

The financial statements are general purpose and are required by section 49 of the *Financial Management and Accountability Act 1997*.

The financial statements have been prepared in accordance with:

- ▶ Finance Minister's Orders (FMOs) for reporting periods ending on or after 1 July 2011;
- ▶ Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial statements have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities at fair value. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position.

The financial statements are presented in Australian dollars and values are rounded to the nearest thousand dollars unless otherwise specified.

Unless an alternative treatment is specifically required by an accounting standard or the FMOs, assets and liabilities are recognised in the Balance Sheet when, and only when, it is probable that future economic benefits will flow to ASIO or a future sacrifice of economic benefits will be required and the amounts of the assets or liabilities can be reliably measured.

However, assets and liabilities arising under agreements equally proportionately unperformed are not recognised unless required by an accounting standard. Liabilities and assets that are unrecognised are reported in the Schedule of Commitments or the Schedule of Contingencies.

Unless alternative treatment is specifically required by an accounting standard, income and expenses are recognised in the Statement of Comprehensive Income when, and only when, the flow or consumption or loss of economic benefits has occurred and can be reliably measured.

### 1.3 Significant Accounting Judgments and Estimates

In the process of applying the accounting policies listed in this note, ASIO has made the following judgments that have the most significant impact on the amounts recorded in the financial statements:

The fair value of land and buildings has been taken to be the market value of similar properties as determined by an independent valuer. In some instances, ASIO buildings are purpose built and may in fact realise more or less in the market.

No accounting assumptions or estimates have been identified that have a significant risk of causing a material adjustment to carrying amounts of assets and liabilities within the next reporting period.

### 1.4 New Australian Accounting Standards

#### Adoption of New Australian Accounting Standard Requirements

No accounting standard has been adopted earlier than the application date as stated in the standard. New standards and amendments to standards that were issued prior to the signing of the statement by the Director-General and are applicable to the current reporting period did not have a financial impact, and are not expected to have a future financial impact on the entity.

#### Future Australian Accounting Standard Requirements

New standards, amendments to standards or interpretations that have been issued by the Australian Accounting Standards Board but are effective for future reporting periods are not expected to have a future financial impact on the entity.

### 1.5 Revenue

Revenue from the sale of goods is recognised when:

- ▶ the risks and rewards of ownership have been transferred to the buyer;
- ▶ the seller retains no managerial involvement or effective control over the goods;
- ▶ the revenue and transaction costs incurred can be reliably measured; and
- ▶ it is probable that the economic benefits associated with the transaction will flow to the entity.

Revenue from the rendering of services is recognised by reference to the stage of completion of contracts at the reporting date. The revenue is recognised when:

- ▶ the amount of revenue, stage of completion and transaction costs incurred can be reliably measured; and
- ▶ the probable economic benefits associated with the transaction will flow to the entity.

The stage of completion of contracts at the reporting date is determined by reference to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

Receivables for goods and services, which have 30-day terms, are recognised at nominal amounts due less any impairment allowance amount. Collectability of debts is reviewed at end of reporting period. Allowances are made when collectability of the debt is no longer probable.

### Revenue from Government

Amounts appropriated for departmental output appropriations for the year (adjusted for any formal additions and reductions) are recognised as revenue from government when ASIO gains control of the appropriation, except for certain amounts that relate to activities that are reciprocal in nature, in which case revenue is recognised only when it has been earned.

Appropriations receivable are recognised at their nominal amounts.

## 1.6 Gains

### Resources Received Free of Charge

Resources received free of charge are recognised as gains when, and only when, a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense.

Resources received free of charge are recorded as either revenue or gains depending on their nature.

### Sale of Assets

Gains from disposal of assets are recognised when control of the asset has passed to the buyer.

## 1.7 Transactions with the Government as Owner

### Equity Injections

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) and Departmental Capital Budgets (DCBs) are recognised directly in contributed equity in that year.

### Distributions to Owners

The FMOs require that distributions to owners be debited to contributed equity unless it is in the nature of a dividend.

## 1.8 Employee Benefits

Liabilities for 'short-term employee benefits' (as defined in *AASB 119 Employee Benefits*) and termination benefits due within twelve months of balance date are measured at their nominal amounts.

The nominal amount is calculated with regard to the rates expected to be paid on settlement of the liability.

Other employee benefit liabilities are measured as the net total of the present value of the defined benefit obligation at the end of the reporting period minus the fair value at the end of the reporting period of plan assets (if any) out of which the obligations are to be settled directly.

### Leave

The liability for employee entitlements includes provision for annual leave and long service leave. No provision has been made for sick leave, as all sick leave is non-vesting and the average sick leave taken in future years by employees of ASIO is estimated to be less than the annual entitlement for sick leave.

The leave liabilities are calculated on the basis of employees' remuneration at the estimated salary rates that apply at the time the leave is taken, including ASIO's employer superannuation contribution rates, to the extent that the leave is likely to be taken during service rather than paid out on termination.

The liability for long service leave has been determined by reference to the work of an actuary as at August 2010. The estimate of present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

### Separation and Redundancy

Provision is made for separation and redundancy benefit payments. ASIO recognises a provision for terminations when it has developed a detailed formal plan for the terminations and has informed those employees affected that it will carry out the terminations.

### Superannuation

Staff of ASIO are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), the PSS accumulation plan (PSSap) or other complying superannuation funds.

The CSS and PSS are defined benefit schemes for the Australian government. The PSSap and other complying funds are defined contribution schemes.

The liability for defined benefits is recognised in the financial statements of the Australian government and is settled by the Australian government in due course. This liability is reported by the Department of Finance and Deregulation's administered schedules and notes.

ASIO makes employer contributions to the employees' superannuation scheme at rates determined by an actuary to be sufficient to meet the current cost to the government. ASIO accounts for the contributions as if they were contributions to defined contribution plans.

Superannuation payable as at 30 June represents outstanding contributions for the final fortnight of the year.

## 1.9 Leases

A distinction is made between finance leases and operating leases. Finance leases effectively transfer from the lessor to the lessee substantially all the risks and rewards incidental to ownership of leased assets. An operating lease is a lease that is not a finance lease. In operating leases, the lessor effectively retains substantially all such risks and benefits.

Where an asset is acquired by means of a finance lease, the asset is capitalised at either the fair value of the lease property or, if lower, the present value of minimum lease payments at the inception of the contract and a liability recognised at the same time and for the same amount.

The discount rate used is the interest rate implicit in the lease. Leased assets are amortised over the period of the lease. Lease payments are allocated between the principal component and the interest expense.

Operating lease payments are expensed on a straight line basis which is representative of the pattern of benefits derived from the leased assets.

## 1.10 Cash

Cash is recognised at its nominal amount. Cash includes:

- ▶ cash on hand; and
- ▶ demand deposits in bank accounts with an original maturity of 3 months or less that are readily convertible to known amounts of cash and subject to insignificant risk of changes in value.

## 1.11 Financial Assets

ASIO classifies its financial assets as 'loans and receivables'.

Financial assets are recognised and derecognised upon 'trade date'.

### Effective Interest Method

The effective interest method is a method of calculating the amortised cost of a financial asset and of allocating interest income over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash receipts through the expected life of the financial asset or, where appropriate, a shorter period.

## Receivables

Trade receivables and other receivables that have fixed or determinable payments that are not quoted in an active market are classified as 'loans and receivables'. Receivables are measured at amortised cost using the effective interest method less impairment. Interest is recognised by applying the effective interest rate.

## Impairment of Financial Assets

Financial assets are assessed for impairment at the end of each reporting period.

*Financial assets held at cost* – if there is objective evidence that an impairment loss has been incurred, the amount of the impairment loss is valued at cost.

## 1.12 Financial Liabilities

ASIO classifies its financial liabilities as 'other financial liabilities'. Financial liabilities are recognised and derecognised upon 'trade date'.

### Other Financial Liabilities

Other financial liabilities are initially measured at fair value, net of transaction costs. These liabilities are subsequently measured at amortised cost using the effective interest method, with interest expense recognised on an effective yield basis.

The effective interest method is a method of calculating the amortised cost of a financial liability and of allocating interest expense over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash payments through the expected life of the financial liability or, where appropriate, a shorter period.

Supplier and other payables are recognised at amortised cost. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).

## 1.13 Contingent Liabilities and Contingent Assets

Contingent Liabilities and Contingent Assets are not recognised in the Balance Sheet but are reported in the relevant schedules and notes. They may arise from uncertainty as to the existence of a liability or asset or represent an existing liability or asset in respect of which the amount cannot be reliably measured. Contingent Assets are reported when settlement is probable, but not virtually certain, and contingent liabilities are recognised when settlement is greater than remote.

## 1.14 Acquisition of Assets

Assets are recorded at cost on acquisition except as stated below. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken. Financial assets are initially measured at their fair value plus transaction costs where appropriate.



Assets acquired at no cost, or for nominal consideration, are initially recognised as assets and revenues at their fair value at the date of acquisition, unless acquired as a consequence of restructuring of administrative arrangements. In the latter case, assets are initially recognised as contributions by owners at the amounts at which they were recognised in the transferor's accounts immediately prior to the restructuring.

## 1.15 Property, Plant and Equipment

### Asset Recognition Threshold

Purchases of property, plant and equipment are recognised initially at cost in the Balance Sheet, except for purchases costing less than \$4,000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

The initial cost of an asset includes an estimate of the cost of dismantling and removing the item and restoring the site on which it is located. This is particularly relevant to restoration obligation provisions in property leases taken up by ASIO where there exists an obligation to restore the property to its original condition. These costs are included in the value of ASIO's leasehold improvements with a corresponding provision for the restoration obligation recognised.

### Revaluations

Fair values for each class of asset are determined as shown below:

Asset Class	Fair value measured at:
Land	market selling price
Buildings	market selling price
Leasehold	depreciated replacement cost
Plant and Equipment	market selling price

Following initial recognition at cost, property, plant and equipment are carried at fair value less accumulated depreciation and accumulated impairment losses. Valuations are conducted with sufficient frequency to ensure that the carrying amounts of assets do not materially differ from the assets' fair values as at the reporting date. The regularity of independent valuations depends upon the volatility of movements in market values for the relevant assets.

Revaluation adjustments are made on a class basis. Any revaluation increment is credited to equity under the heading of 'asset revaluation surplus' except to the extent that it reverses a previous revaluation decrement of the same asset class that was previously recognised in the surplus/deficit. Revaluation decrements for a class of assets are recognised directly in the surplus/deficit except to the extent that they reverse a previous revaluation increment for that class.

Any accumulated depreciation as at the revaluation date is eliminated against the gross carrying amount of the asset and the asset restated to the revalued amount.

## Depreciation

Depreciable property, plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to ASIO using, in all cases, the straight-line method of depreciation. Leasehold improvements are depreciated on a straight-line basis over the lesser of the estimated useful life of the improvements or the unexpired period of the lease.

Depreciation rates (useful lives), residual values and methods are reviewed at each reporting date and necessary adjustments are recognised in the current or current and future reporting periods, as appropriate.

Depreciation rates applying to each class of depreciable asset are based on the following useful lives:

	2013	2012
Buildings on freehold land	<b>3–40 years</b>	25–40 years
Leasehold improvements	<b>lease term</b>	lease term
Plant and equipment	<b>2–21 years</b>	2–20 years

## Impairment

All assets were assessed for impairment at 30 June 2013. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment made if the asset's recoverable amount is less than its carrying amount.

The recoverable amount of an asset is the higher of its fair value less costs to sell and its value in use. Value in use is the present value of the future cash flows expected to be derived from the asset. Where the future economic benefit of an asset is not primarily dependent on the asset's ability to generate future cash flows, and the asset would be replaced if ASIO were deprived of the asset, its value in use is taken to be its depreciated replacement cost.

## Derecognition

An asset is derecognised upon disposal or when no further future economic benefits are expected from its use or disposal.

### 1.16 Intangibles

ASIO's intangibles comprise internally developed and purchased software for internal use. These assets are carried at cost less accumulated amortisation and accumulated impairment losses.

Software is amortised on a straight-line basis over its anticipated useful life. The useful life of ASIO's software is 1–10 years (2011–12: 4–5 years).

All software assets were assessed for indications of impairment as at 30 June 2013.

## 1.17 Taxation

ASIO is exempt from all forms of taxation except fringe benefits tax and the goods and services tax (GST).

Revenues, expenses and assets are recognised net of GST:

- ▶ except where the amount of GST incurred is not recoverable from the Australian Taxation Office; and
- ▶ except for receivables and payables.

## 1.18 Legal

The Australian government continues to have regard to developments in case law, including the High Court's most recent decision on Commonwealth expenditure in *Williams v Commonwealth* (2012) 288 ALR410, as they contribute to the larger body of law relevant to the development of Commonwealth programs.

In accordance with its general practice, the government will continue to monitor and assess risk and decide on any appropriate actions to respond to risks of expenditure not being consistent with constitutional or other legal requirements.

## Note 2: Events after the Balance Sheet Date

On 13 August 2013 the *Instrument to Reduce Appropriations (No. 1 of 2013–2014)* signed by the Minister for Finance and Deregulation took effect. The instrument gave legal standing to the reduction of ASIO's Appropriation Act (No. 1) 2012–2013 by \$10,226,000. The result of this reduction is reflected in the Statement of Comprehensive Income and Balance Sheet. As required by the FMOs, the reduction is not included in Notes 14A Annual Appropriations and 14C Unspent departmental annual appropriations. The instrument would have the effect of reducing:

- ▶ in Note 5A: *Appropriations receivable for existing programs* and the corresponding *Trade and Other Receivables* in the Balance Sheet by \$10,226,000;
- ▶ in Note 7C: *Payable to government (appropriation)* and the corresponding *Other Payables* in the Balance Sheet by \$10,226,000;
- ▶ in Note 14A: *Departmental ordinary annual services* by \$10,226,000; and
- ▶ in Note 14C: *Appropriation Act (No. 1) 2012–13* by \$10,226,000,

if it had been executed in the 2012-13 financial year.

2012: On 22 August 2012 the Director-General of Security announced a voluntary redundancy program targeted at Senior Executive Service officers. At the date of signing the 2012 financial statements, none had been finalised and the financial effect was unknown. The financial effect is shown in the 2013 statements.

## Note 3: Expenses

	2013	2012
	\$ '000	\$ '000

### Note 3A: Employee benefits

Wages and salaries	164,117	156,495
Superannuation:		
Defined contribution plans	13,355	11,074
Defined benefit plans	18,219	15,808
Leave and other entitlements	13,737	23,126
Separation and redundancies	3,647	1,883
<b>Total employee benefits</b>	<b>213,075</b>	<b>208,386</b>

### Note 3B: Suppliers

Provision of goods — related entities	285	664
Provision of goods — external entities	6,647	7,528
Rendering of services — related entities	22,072	26,638
Rendering of services — external entities	80,280	88,798
Operating lease rentals — related entities:		
minimum lease payments	3,943	3,850
Operating lease rentals — external entities:		
minimum lease payments	17,631	16,378
Workers' compensation premiums	1,985	2,443
<b>Total supplier expenses</b>	<b>132,843</b>	<b>146,299</b>

### Note 3C: Depreciation and amortisation

Depreciation		
Property, plant and equipment	28,465	23,403
Buildings	21,295	11,525
<b>Total depreciation</b>	<b>49,760</b>	<b>34,928</b>
<b>Amortisation — Intangibles — computer software</b>	<b>6,661</b>	<b>5,245</b>
<b>Total depreciation and amortisation</b>	<b>56,421</b>	<b>40,173</b>

### Note 3D: Finance costs

<b>Unwinding of discount — restoration obligations</b>	<b>179</b>	<b>807</b>
--	------------	------------

2013	2012
\$ '000	\$ '000

### Note 3E: Write-down and impairment of assets

Asset write-downs and impairments from:

Impairment of receivables	6,858	21
Revaluation decrement of property, plant and equipment	1,622	-
Write-down of property, plant and equipment	2,540	355
Write-down of intangible assets	38	58
<b>Total write-down and impairment of assets</b>	<b>11,058</b>	<b>434</b>

### Note 3F: Losses from asset sales

Property, plant and equipment

Proceeds from sale	(729)	(884)
Carrying value of assets sold	890	1,021
<b>Total losses from asset sales</b>	<b>161</b>	<b>137</b>

## Note 4: Income

### OWN SOURCE REVENUE

#### Note 4A: Sale of goods and rendering of services

Provision of goods — related entities	8	12
Provision of goods — external entities	4	7
Rendering of services — related entities	25,341	18,063
Rendering of services — external entities	2,212	3,000
<b>Total sale of goods and rendering of services</b>	<b>27,565</b>	<b>21,082</b>

### GAINS

#### Note 4B: Rental income

<b>Rental income – operating lease</b>	<b>1,007</b>	<b>1,306</b>
--	--------------	--------------

#### Note 4C: Other

Resources received free of charge	115	115
Other	375	117
<b>Total other gains</b>	<b>490</b>	<b>232</b>

### REVENUE FROM GOVERNMENT

#### Note 4D: Revenue from government

<b>Appropriation — Departmental appropriations</b>	<b>329,743</b>	<b>328,124</b>
--	----------------	----------------

## Note 5: Financial Assets

	2013	2012
	\$ '000	\$ '000

### Note 5A: Trade and other receivables

Goods and services

Related entities	1,406	5,497
External entities	663	246
<b>Total receivables for goods and services</b>	<b>2,069</b>	<b>5,743</b>
Appropriations receivable for existing programs	200,676	226,225
GST receivable from the Australian Taxation Office	2,303	2,215
<b>Total trade and other receivables (gross)</b>	<b>205,048</b>	<b>234,183</b>
Less impairment allowance account:	-	-
<b>Total trade and other receivables (net)</b>	<b>205,048</b>	<b>234,183</b>

All receivables are expected to be recovered in no more than 12 months.

Receivables are aged as follows:

Not overdue	203,957	231,437
Overdue by:		
less than 30 days	358	589
31 to 60 days	149	63
61 to 90 days	98	1,874
more than 90 days	486	220
<b>Total receivables (gross)</b>	<b>205,048</b>	<b>234,183</b>

### Note 5B: Other financial assets

<b>Accrued revenue</b>	<b>6,178</b>	<b>4,378</b>
------------------------	--------------	--------------

All accrued revenue is expected to be recovered in no more than 12 months.

## Note 6: Non-Financial Assets

	2013	2012
	\$ '000	\$ '000

### Note 6A: Land and buildings

<b>Land at fair value</b>	<b>1,565</b>	1,515
<b>Buildings on freehold land</b>		
fair value	5,635	7,746
accumulated depreciation	(109)	(1,192)
<b>Total buildings on freehold land</b>	<b>5,526</b>	6,554
<b>Leasehold improvements</b>		
work in progress	212,140	150,074
fair value	50,010	78,139
accumulated depreciation	(3,983)	(23,587)
<b>Total leasehold improvements</b>	<b>258,167</b>	204,626
<b>Total land and buildings (non-current)</b>	<b>265,258</b>	212,695

No indicators of impairment were found for land and buildings.

No land and buildings are expected to be sold or disposed of within the next 12 months.

### Note 6B: Property, plant and equipment

#### Property, plant and equipment

work in progress	1,615	139
fair value	83,706	126,713
accumulated depreciation	(6,577)	(48,073)
<b>Total property, plant and equipment (non-current)</b>	<b>78,744</b>	78,779

No indicators of impairment were found for infrastructure, plant and equipment.

Property, plant and equipment of an immaterial value only is expected to be sold or disposed of within the next 12 months.

#### Revaluations of non-financial assets

All revaluations were conducted in accordance with the revaluation policy stated in Note 1.

On 31 March 2013, an independent valuer conducted the revaluations.

Revaluation amounts were:

Land and buildings – increment transferred to asset revaluation surplus	10,441	–
Property, plant and equipment – decrement transferred to asset revaluation surplus	(449)	–
Property, plant and equipment – decrement expensed	(1,622)	–

	2013	2012
	\$ '000	\$ '000

## Note 6C: Intangibles

### Computer software

purchased	21,486	16,827
internally developed — in progress	1,831	1,892
internally developed — in use	24,606	23,313
accumulated amortisation	(28,482)	(25,467)
accumulated impairment	(82)	(1,125)
<b>Total computer software</b>	<b>19,359</b>	<b>15,440</b>
<b>Total intangibles (non-current)</b>	<b>19,359</b>	<b>15,440</b>

No indicators of impairment were found for intangibles.



Note 6D: Reconciliation of the opening and closing balances of property, plant and equipment

	Land \$'000	Buildings \$'000	Buildings – leasehold improvement \$'000	Property, plant & equipment \$'000	Total \$'000
<b>2013</b>					
<b>As at 1 July 2012</b>					
Gross book value	1,515	7,746	228,213	126,852	364,326
Accumulated depreciation and impairment	-	(1,192)	(23,587)	(48,073)	(72,852)
<b>Net book value 1 July 2012</b>	<b>1,515</b>	<b>6,554</b>	<b>204,626</b>	<b>78,779</b>	<b>291,474</b>
Additions by purchase	-	-	63,421	33,932	97,353
Revaluations and impairments recognised in other comprehensive income	50	210	10,181	(450)	9,991
Revaluations recognised in the operating result	-	-	-	(1,622)	(1,622)
Depreciation expense	-	(1,239)	(20,056)	(28,465)	(49,760)
Disposals – other	-	-	(4)	(3,683)	(3,687)
Depreciation Adjustment	-	-	-	254	254
<b>Net book value 30 June 2013</b>	<b>1,565</b>	<b>5,525</b>	<b>258,168</b>	<b>78,744</b>	<b>344,002</b>
<b>Net book value 30 June 2013 represented by:</b>					
Gross book value	1,565	5,635	262,150	85,321	354,671
Accumulated depreciation and impairment	-	(109)	(3,983)	(6,577)	(10,669)
	<b>1,565</b>	<b>5,525</b>	<b>258,168</b>	<b>78,744</b>	<b>344,002</b>
<b>2012</b>					
<b>As at 1 July 2011</b>					
Gross book value	1,515	7,653	116,381	107,013	232,562
Accumulated depreciation and impairment	-	(530)	(13,054)	(25,547)	(39,131)
<b>Net book value 1 July 2011</b>	<b>1,515</b>	<b>7,123</b>	<b>103,328</b>	<b>81,466</b>	<b>193,431</b>
Additions by purchase	-	93	112,161	22,092	134,346
Depreciation expense	-	(662)	(10,863)	(23,403)	(34,928)
Disposals – other	-	-	-	(1,377)	(1,377)
<b>Net book value 30 June 2012</b>	<b>1,515</b>	<b>6,554</b>	<b>204,626</b>	<b>78,779</b>	<b>291,474</b>
<b>Net book value as at 30 June 2012 represented by:</b>					
Gross book value	1,515	7,746	228,213	126,852	364,326
Accumulated depreciation and impairment	-	(1,192)	(23,587)	(48,073)	(72,852)
	<b>1,515</b>	<b>6,554</b>	<b>204,626</b>	<b>78,779</b>	<b>291,474</b>

## Note 6E: Reconciliation of the opening and closing balances of intangibles

	Computer software		
	Internally developed	Purchased	Total
	\$'000	\$'000	\$'000

### 2013

#### As at 1 July 2012

Gross book value	25,205	16,827	42,032
Accumulated amortisation and impairment	(14,669)	(11,923)	(26,592)
<b>Net book value 1 July 2012</b>	<b>10,536</b>	<b>4,904</b>	<b>15,440</b>

Additions by purchase or internally developed	4,618	6,001	10,619
Amortisation expense	(4,220)	(2,441)	(6,661)
Disposals — other	–	(38)	(38)
<b>Net book value 30 June 2013</b>	<b>10,934</b>	<b>8,426</b>	<b>19,359</b>

#### Net book value 30 June 2013 represented by:

Gross book value	26,437	21,486	47,923
Accumulated amortisation and impairment	(15,503)	(13,061)	(28,564)
	<b>10,934</b>	<b>8,426</b>	<b>19,359</b>

### 2012

#### As at 1 July 2011

Gross book value	14,964	13,602	28,566
Accumulated amortisation and impairment	(11,418)	(10,264)	(21,682)
<b>Net book value 1 July 2011</b>	<b>3,546</b>	<b>3,338</b>	<b>6,884</b>

Additions by purchase or internally developed	10,241	3,617	13,858
Amortisation expense	(3,250)	(1,994)	(5,245)
Disposals – other	–	(58)	(58)
<b>Net book value 30 June 2012</b>	<b>10,536</b>	<b>4,904</b>	<b>15,440</b>

#### Net book value 30 June 2012 represented by:

Gross book value	25,205	16,827	42,032
Accumulated amortisation and impairment	(14,669)	(11,923)	(26,592)
	<b>10,536</b>	<b>4,904</b>	<b>15,440</b>

## Note 6F: Other non-financial assets

	2013	2012
	\$ '000	\$ '000
Prepayments	14,640	15,503
<b>Total other non-financial assets</b>	<b>14,640</b>	<b>15,503</b>

Total other non-financial assets are expected to be recovered in:

No more than 12 months	9,290	13,993
More than 12 months	5,350	1,510
	<b>14,640</b>	<b>15,503</b>

No indicators of impairment were found for other non-financial assets.

## Note 7: Payables

### Note 7A: Suppliers

<b>Trade creditors and accruals</b>	<b>14,026</b>	<b>14,785</b>
-------------------------------------	---------------	---------------

Supplier payables expected to be settled within 12 months:

Related entities	513	3,562
External entities	13,513	11,223
	<b>14,026</b>	<b>14,785</b>

Settlement is usually made within 30 days.

### Note 7B: Lease incentives

<b>Lease incentives</b>	<b>2,201</b>	<b>2,756</b>
-------------------------	--------------	--------------

Lease incentives are expected to be settled in:

No more than 12 months	601	588
More than 12 months	1,600	2,168
	<b>2,201</b>	<b>2,756</b>

### Note 7C: Other payables

Salaries and wages	4,559	4,241
Superannuation	861	778
Unearned income	115	110
Fringe benefits tax	69	856
Rent payable	4,484	3,312
Payable to government (appropriation)	10,226	-
<b>Total other payables</b>	<b>20,314</b>	<b>9,297</b>

Rent payable is expected to be settled over properties' various remaining lease terms (0 to 7 years). All other payables are expected to be settled in no more than 12 months.

## Note 8: Provisions

	2013	2012
	\$ '000	\$ '000

### Note 8A: Employee provisions

Leave	57,643	57,465
Redundancies	-	520
Superannuation	442	882
<b>Total employee provisions</b>	<b>58,085</b>	<b>58,867</b>

Employee provisions are expected to be settled in:

No more than 12 months	39,921	40,194
More than 12 months	18,164	18,673
	<b>58,085</b>	<b>58,867</b>

### Note 8B: Restoration obligations

<b>Restoration obligations</b>	<b>10,024</b>	<b>9,979</b>
--------------------------------	---------------	--------------

Restoration obligations are expected to be settled in:

No more than 12 months	4,127	260
More than 12 months	5,897	9,719
	<b>10,024</b>	<b>9,979</b>

Carrying amount 1 July 2012	9,979	7,105
Additional provisions	38	-
Lease expiry	(336)	-
Revaluations	164	2,067
Unwinding of discount or change in discount rate	179	807
<b>Closing balance</b>	<b>10,024</b>	<b>9,979</b>

ASIO currently has agreements for the leasing of premises which have provisions requiring ASIO to restore the premises to their original condition at the conclusion of the lease. ASIO has made a provision to reflect the present value of this obligation.

## Note 9: Cash Flow Reconciliation

	2013	2012
	\$ '000	\$ '000

### Reconciliation of cash and cash equivalents as per balance sheet to cash flow statement

#### Cash and cash equivalents as per:

Cash Flow Statement	14,217	12,775
Balance Sheet	14,217	12,775

#### Reconciliation of net cost of services to net cash from operating activities:

Net cost of services	(384,674)	(373,618)
Add revenue from government	329,743	328,124

#### Adjustments for non-cash items

Depreciation/amortisation	56,421	40,173
Net write-down of non-financial assets	2,578	413
Net loss on disposal of assets	161	137
Revaluation of property, plant and equipment	1,622	-
Revaluation of restoration obligation liabilities	(164)	-

#### Changes in assets/liabilities

(Increase)/decrease in receivables	29,134	77,057
(Increase)/decrease in accrued revenue	(1,800)	(3,784)
(Increase)/decrease in prepayments	863	(1,359)
Increase/(decrease) in employee provisions	(781)	13,395
Increase/(decrease) in restoration obligations	45	2,874
Increase/(decrease) in lease incentives	(555)	(556)
Increase/(decrease) in supplier payables	(2,886)	4,744
Increase/(decrease) in other payables	11,017	(964)
<b>Net cash from/(used by) operating activities</b>	<b>40,724</b>	<b>86,636</b>

## Note 10: Contingent Liabilities and Assets

### Quantifiable contingencies

The schedule of contingencies reports \$210,000 of contingent liabilities in respect of claims for damages or costs (2012: Nil). The amount represents an estimate of ASIO's liability based on precedent in such cases. ASIO is defending the claims.

### Unquantifiable contingencies

At 30 June 2013, ASIO had a number of legal claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate amounts of any eventual payments that may be required in relation to these claims (2012: Nil).

### Significant remote contingencies

ASIO does not have any significant remote contingencies.

## Note 11: Remuneration of Auditors

	2013	2012
	\$	\$

Financial statement audit services are provided free of charge to ASIO by the Australian National Audit Office. No other services were provided by the Auditor-General.

Fair value	<b>115,000</b>	115,000
------------	----------------	---------

## Note 12: Senior Executive Remuneration

	2013	2012
	\$	\$

### Note 12A: Senior executive expense for the reporting period

Short-term employee benefits:

Salary	<b>11,016,713</b>	11,465,960
Annual leave accrued	<b>890,174</b>	941,931
Performance bonuses	-	-
Motor vehicle and other allowances	<b>922,185</b>	1,427,044
<b>Total short-term employee benefits</b>	<b>12,829,072</b>	13,834,935

Post-employment benefits

Superannuation	<b>2,195,623</b>	2,383,594
----------------	------------------	-----------

Other long-term benefits

Long-service leave accrued	<b>290,234</b>	308,613
----------------------------	----------------	---------

Termination benefits	<b>4,083,979</b>	247,197
<b>Total</b>	<b>19,398,908</b>	16,774,339

Note 12A includes the portion of employees' remuneration relating to Senior Executive Service acting arrangements and part-year services where their total remuneration for the year is greater than \$180,000.

Note 12A is prepared on an accrual basis and therefore performance bonus expenses disclosed will differ from the cash 'bonus paid' in note 12B.

## Note 12B: Average annual reportable remuneration paid to substantive senior executives during the reporting period

Average annual reportable remuneration	Senior executives No.	Reportable salary \$	Contributed superannuation \$	Bonus paid \$	Total \$
<b>2013</b>					
Total remuneration:					
\$0 to \$179,999	3	73,754	21,201	–	94,955
\$180,000 to \$209,999	3	169,317	24,902	–	194,219
\$210,000 to \$239,999	10	190,178	40,400	–	230,578
\$240,000 to \$269,999	21	200,330	52,612	–	252,942
\$270,000 to \$299,999	10	230,497	52,262	–	282,759
\$300,000 to \$329,999	5	265,091	46,428	–	311,519
\$330,000 to \$359,999	3	290,652	49,392	–	340,044
\$360,000 to \$389,999	2	305,537	70,417	–	375,954
\$420,000 to \$449,999	1	397,239	32,435	–	429,674
\$540,000 to \$569,999	1	446,695	110,067	–	556,762
<b>Total</b>	<b>59</b>				

2012

Total remuneration:

\$0 to \$179,000	7	68,950	16,776	5,120	90,846
\$180,000 to \$209,999	2	159,426	29,675	7,041	196,143
\$210,000 to \$239,999	15	185,570	39,049	6,731	231,350
\$240,000 to \$269,999	26	188,794	52,164	8,491	249,449
\$270,000 to \$299,999	11	224,600	57,604	11,039	293,243
\$300,000 to \$329,999	2	239,326	63,734	10,845	313,905
\$360,000 to \$389,999	2	279,973	77,961	9,455	367,389
\$510,000 to \$539,999	1	404,974	116,690	–	521,664
<b>Total</b>	<b>66</b>				

This table reports substantive senior executives who received remuneration during the reporting period. Each row is an averaged figure based on headcount for individuals in that band.

Reportable salary includes gross payments as reported on employees' payment summaries (less bonuses paid, which are separated out and disclosed in the 'bonus paid' column), salary sacrificed benefits and reportable fringe benefits (at the net amount prior to 'grossing up' for tax purposes).

The contributed superannuation amount is the average cost to ASIO for the provision of superannuation benefits to substantive senior executives in that reportable remuneration band during the reporting period.

Bonus paid represents average actual bonuses paid during the reporting period in that reportable remuneration band.

Various salary sacrifice arrangements were available to senior executives including superannuation, motor vehicle and expense payment fringe benefits. Salary sacrifice benefits are reported in the reportable salary column.

There were no reportable allowances.



## Note 12C: Other highly paid staff

Average annual reportable remuneration	Staff No.	Reportable salary \$	Contributed superannuation \$	Bonus paid \$	Total \$
--	-----------	----------------------	-------------------------------	---------------	----------

### 2013

Total remuneration:

\$180,000 to \$209,999	38	152,134	38,653	-	190,787
\$210,000 to \$239,999	10	180,405	39,876	-	220,281
\$240,000 to \$269,999	1	201,685	45,852	-	247,537
<b>Total</b>	<b>49</b>				

### 2012

Total remuneration:

\$180,000 to \$209,999	19	150,105	39,298	1,387	190,790
\$210,000 to \$239,999	6	176,604	38,919	2,325	217,848
<b>Total</b>	<b>25</b>				

This table reports staff:

- ▶ who were employed by ASIO during the reporting period;
- ▶ whose reportable remuneration was \$180,000 or more for the reporting period; and
- ▶ were not required to be disclosed in Table B.

Each row is an averaged figure based on headcount for individuals in that band.

Reportable salary includes gross payments (less bonuses paid, which are separated out and disclosed in the 'bonus paid' column), salary sacrificed benefits and reportable fringe benefits (at the net amount prior to 'grossing up' for tax purposes).

The contributed superannuation amount is the average cost to ASIO for the provision of superannuation benefits to staff in that reportable remuneration band during the reporting period.

Bonus paid represents average actual bonuses paid during the reporting period in that reportable remuneration band.

Various salary sacrifice arrangements were available to other highly paid staff including superannuation, motor vehicle and expense payment fringe benefits. Salary sacrifice benefits are reported in the reportable salary column.

There were no reportable allowances.

## Note 13: Financial Instruments

	2013	2012
	\$'000	\$'000

### Note 13A: Categories of financial instruments

#### Financial assets

Loans and receivables

Cash	14,217	12,775
Trade receivables	2,069	5,743
Accrued revenue	6,178	4,378
<b>Carrying amount of financial assets</b>	<b>22,464</b>	<b>22,896</b>

#### Financial liabilities

At amortised cost

Trade creditors and accruals	14,026	14,785
<b>Carrying amount of financial liabilities</b>	<b>14,026</b>	<b>14,785</b>

### Note 13B: Net income and expense from financial assets

There is no net income from financial assets through the profit and loss for the period ending 30 June 2013 (2012: Nil).

The total expense from financial assets through the profit and loss for the period ending 30 June 2013 was \$6,858,471 (2012: \$20,619).

### Note 13C: Net income and expense from financial liabilities

There is no net income and expense from financial liabilities through profit or loss for the period ending 30 June 2013 (2012: Nil).

## Note 13D: Fair value of financial instruments

	2013 \$'000	2013 \$'000	2012 \$'000	2012 \$'000
	Carrying amount	Fair value	Carrying amount	Fair value
<b>Financial assets</b>				
Loans and receivables				
Cash	14,217	14,217	12,775	12,775
Trade receivables	2,069	2,069	5,743	5,743
Accrued revenue	6,178	6,178	4,378	4,378
<b>Total</b>	<b>22,464</b>	<b>22,464</b>	22,896	22,896
<b>Financial liabilities</b>				
At amortised cost				
<b>Trade creditors and accruals</b>	<b>14,026</b>	<b>14,026</b>	14,785	14,785

## Note 13E: Credit risk

ASIO's maximum exposures to credit risk at the reporting date in relation to each class of recognised financial assets is the carrying amount of those assets as indicated in the Balance Sheet.

ASIO is exposed to minimal credit risk in relation to potential debtor default. ASIO provides for this risk through the recognition of an allowance for impairment where necessary.

ASIO manages its debtors by undertaking recovery processes for those receivables which are considered to be overdue. The risk of overdue debts arising is negated through the implementation of credit assessments on potential customers.

ASIO's credit risk profile has not changed from the prior financial year.

The following table illustrates ASIO's gross exposure to credit risk, excluding any collateral or credit enhancements.

	2013	2012
	\$'000	\$'000
<b>Financial assets</b>		
Loans and receivables		
Cash	14,217	12,775
Trade receivables	2,069	5,743
Accrued revenue	6,178	4,378
<b>Total financial assets</b>	<b>22,464</b>	<b>22,896</b>
<b>Financial liabilities</b>		
At amortised cost		
<b>Trade creditors and accruals</b>	<b>14,026</b>	<b>14,785</b>

The credit quality of financial instruments not past due or individually determined as impaired:

	2013	2012	2013	2012
	\$'000	\$'000	\$'000	\$'000
	Not past due nor impaired		Past due or impaired	
Loans and receivables				
Cash <sup>1</sup>	14,217	12,775	-	-
Trade receivables <sup>2</sup>	977	2,997	1,091	2,746
Accrued revenue <sup>3</sup>	6,178	4,378	-	-
<b>Total loans and receivables</b>	<b>21,372</b>	<b>20,150</b>	<b>1,091</b>	<b>2,746</b>

<sup>1</sup> Cash is subject to minimal credit risk, as cash holdings are held with the Reserve Bank of Australia.

<sup>2</sup> Trade and other receivables are subject to minimal credit risk, the majority of which will be recovered on a timely basis.

<sup>3</sup> Accrued revenue is subject to minimal credit risk as full recovery is expected.

## Ageing of financial assets that are past due but not impaired

	0 to 30 days	31 to 60 days	61 to 90 days	90+ days	Total
	\$'000	\$'000	\$'000	\$'000	\$'000

### 2013

Loans and receivables

<b>Trade and other receivables</b>	<b>358</b>	<b>149</b>	<b>98</b>	<b>486</b>	<b>1,091</b>
------------------------------------	------------	------------	-----------	------------	--------------

2012

Loans and receivables

<b>Trade and other receivables</b>	<b>589</b>	<b>63</b>	<b>1,874</b>	<b>220</b>	<b>2,746</b>
------------------------------------	------------	-----------	--------------	------------	--------------

## Note 13F: Liquidity risk

ASIO has no significant exposures to any concentrations of liquidity risk.

ASIO analyses measures of liquidity, such as the relationship between current assets and current liabilities. Such processes, together with the application of full cost recovery, ensure that at any point in time ASIO has appropriate resources available to meet its financial obligations as and when they fall due.

ASIO manages liquidity risk by ensuring all financial liabilities are paid in accordance with terms and conditions on demand. ASIO's liquidity risk profile has not changed from 2010–11.

The following table illustrates the maturities for financial liabilities.

	On demand	within 1 year	1 to 5 years	> 5 years	Total
	\$'000	\$'000	\$'000	\$'000	\$'000

### 2013

At amortised cost

<b>Trade creditors and accruals</b>	<b>-</b>	<b>14,026</b>	<b>-</b>	<b>-</b>	<b>14,026</b>
-------------------------------------	----------	---------------	----------	----------	---------------

2012

At amortised cost

<b>Trade creditors and accruals</b>	<b>-</b>	<b>14,785</b>	<b>-</b>	<b>-</b>	<b>14,785</b>
-------------------------------------	----------	---------------	----------	----------	---------------

## Note 13G: Market risk

ASIO holds basic financial instruments that do not expose it to certain market risks. ASIO's market risk profile has not changed from 2010–11. ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

## Note 14: Appropriations

### Note 14A: Annual appropriations

	Appropriation Act		FMA Act		Total appropriation	Appropriation applied in 2013	
	Annual appropriation	Section 30	Section 31 (GST excl.)	Total appropriation		(current and prior years)	Variance
	\$ '000	\$ '000	\$ '000	\$ '000		\$ '000	\$ '000

#### 2013

##### Departmental

Ordinary annual services	400,735	3,518	29,297	433,550	(460,716)	(27,166)
--------------------------	---------	-------	--------	---------	-----------	----------

##### Other services

Equity	5,062	-	-	5,062	-	5,062
--------	-------	---	---	-------	---	-------

<b>Total Departmental</b>	<b>405,797</b>	<b>3,518</b>	<b>29,297</b>	<b>438,612</b>	<b>(460,716)</b>	<b>(22,104)</b>
---------------------------	----------------	--------------	---------------	----------------	------------------	-----------------

#### 2012

##### Departmental

Ordinary annual services	347,352	12,346	19,856	379,554	(409,476)	(29,922)
--------------------------	---------	--------	--------	---------	-----------	----------

##### Other services

Equity	41,806	-	-	41,806	(90,505)	(48,699)
--------	--------	---	---	--------	----------	----------

<b>Total Departmental</b>	<b>389,158</b>	<b>12,346</b>	<b>19,856</b>	<b>421,360</b>	<b>(499,981)</b>	<b>(78,621)</b>
---------------------------	----------------	---------------	---------------	----------------	------------------	-----------------

## Note 14B: Departmental Capital Budgets

	Appropriation Act	Appropriations applied	
	Annual Capital Budget	Payments for non-financial assets	Variance
	\$ '000	\$ '000	\$ '000

### 2013

#### Departmental

Ordinary annual services

Departmental Capital Budget	60,766	(8,360)	52,406
<b>Total Departmental</b>	<b>60,766</b>	<b>(8,360)</b>	<b>52,406</b>

### 2012

#### Departmental

Ordinary annual services

Departmental Capital Budget	19,228	(12,228)	7,000
<b>Total Departmental</b>	<b>19,228</b>	<b>(12,228)</b>	<b>7,000</b>

Departmental Capital Budgets are appropriated through Appropriation Acts (No. 1, 3, 5). They form part of ordinary annual services, and are not separately identified in the Appropriation Acts.

Payments made for non-financial assets include purchases of assets and expenditure on assets which have been capitalised.

## Note 14C: Unspent departmental annual appropriations

	2013	2012
	\$ '000	\$ '000
Appropriation Act (No.1) 2012-13	207,952	-
Appropriation Act (No.2) 2012-13	5,062	-
Appropriation Act (No.1) 2011-12	1,879	239,002
<b>Total</b>	<b>214,893</b>	<b>239,002</b>

## Note 14D: Disclosure by agent in relation to annual appropriations

	2013		2012	
	DoFD	DFAT	DoFD	DFAT
	\$ '000	\$ '000	\$ '000	\$ '000
<b>Total payments</b>	<b>59,309</b>	<b>11,545</b>	90,505	13,295

Agent payments to the Department of Finance and Deregulation relate to the construction of a new building.

Agent payments to the Department of Foreign Affairs and Trade relate to services overseas.

## Note 15: Compensation and Debt Relief

	2013	2012
	\$ '000	\$ '000

### Compensation and Debt Relief - Departmental

Act of Grace payments	-	-
Waivers of amounts owing to the Australian government pursuant to subsection 34(1) of the <i>Financial Management and Accountability Act 1997</i>	-	-
Payments made under the Compensation for Detriment caused by Defective Administration (CDDA) Scheme	-	-
Ex-gratia payments	-	-

## Note 16: Reporting of Outcomes

	2013	2012
	\$ '000	\$ '000

### Expenses

Departmental	<b>413,736</b>	396,238
--------------	----------------	---------

### Income from non-government sector

Departmental		
Activities subject to cost recovery	<b>(2,216)</b>	(3,007)
Other	<b>(375)</b>	(254)
	<b>(2,591)</b>	(3,261)

### Other own-source income

Departmental	<b>(26,471)</b>	(19,452)
<b>Net cost of outcome delivery</b>	<b>384,674</b>	373,525

Net costs shown include intra-government costs that are eliminated in calculating the actual Budget Outcome.



## Note 17: Net Cash Appropriation Arrangements

	2013	2012
	\$ '000	\$ '000
Total comprehensive income (loss) plus depreciation and amortisation expenses previously funded through revenue appropriations	11,318	(5,321)
Less depreciation and amortisation expenses previously funded through revenue appropriation	(56,421)	(40,173)
<b>Total comprehensive loss as per statement of comprehensive income</b>	<b>(45,103)</b>	<b>(45,494)</b>

From 2010–11, the government introduced net cash appropriation arrangements, where revenue appropriations for depreciation and amortisation expenses ceased. Entities now receive a separate capital budget provided through equity appropriations. Capital budgets are to be appropriated in the period when cash payment for capital expenditure is required.





# Part 7

## APPENDICES AND INDICES

‘The task of the Director-General of Security is to ensure ASIO, operating in the secret but real world of counter-terrorism and counter-espionage, is taking all necessary steps to protect the security and safety of Australians and our democratic institutions, while at the same time ensuring the appropriate protection of individual civil liberties.’

► *Speech by the Director-General to the Biennial Conference of the District and County Court Judges [of Australia and New Zealand]  
26 June 2013*

# Appendix A

## Agency Resource Statement

	Actual available appropriation for	Payments made	Balance remaining
	2012–13	2012–13	2012–13
	\$'000	\$'000	\$'000

### Ordinary annual services<sup>5</sup>

#### Departmental appropriation<sup>2</sup>

Prior year departmental appropriation	226,227*	224,348	1,879
Departmental appropriation <sup>1</sup>	398,009*	207,000	191,009
Appropriation quarantined	2,726	–	2,726
s31 relevant agency receipts <sup>4</sup>	29,297	27,292	2,005
s31 relevant agency receipts			
June 2012 receipts not redrawn until July 2012			(2,005)
s30 FMA Act	3,518	3,518	–
Cash on hand		6,110	14,217
<b>Total ordinary annual services</b>	<b>659,777</b>	<b>468,268</b>	<b>209,831</b>

### Other services

#### Departmental non-operating<sup>3</sup>

Equity injections	5,062	–	5,062
<b>Total other services</b>	<b>5,062</b>	<b>–</b>	<b>5,062</b>
<b>Total net resourcing and payments for ASIO</b>	<b>664,839</b>	<b>468,268</b>	

<sup>1</sup> Appropriation Bill (No.1) 2012–13

<sup>2</sup> Includes an amount of \$60.766m in 2012–13 for the departmental capital budget. For accounting purposes this amount has been designated as 'contributions by owners'.

<sup>3</sup> Appropriation Bill (No.2) 2012–13

<sup>4</sup> \$32.318m per Portfolio Budget Statement less \$3.021m overestimate at time of Portfolio Budget Statements (PBS)

<sup>5</sup> Due to specifications in the Department of the Prime Minister and Cabinets' Requirements for Annual Reports, various elements of the Ordinary annual services will not always sum across the columns.

\* as per PBS

# Appendix B

## Expenses by outcomes

	Budget*	Actual expenses	Variation
	2012-13	2012-13	2012-13
	\$'000	\$'000	\$'000

### Outcome 1:

**To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government**

#### Program 1.1: Security Intelligence

Departmental expenses

Departmental appropriation	369,561	357,200	12,361
Expenses not requiring appropriation in the Budget year	46,765	56,536	(9,771)
<b>Total for Program 1.1</b>	<b>416,326</b>	<b>413,736</b>	<b>2,590</b>
<b>Total expenses for Outcome 1</b>	<b>416,326</b>	<b>413,736</b>	<b>2,590</b>

\* as per Portfolio Budget Statements

	2011-12	2012-13	Variation
<b>Average staffing levels numbers</b>	<b>1,683</b>	<b>1,739</b>	<b>56</b>

## Appendix C

### Mandatory reporting requirements for Questioning Warrants and for Questioning and Detention Warrants under section 94 of the ASIO Act

Section	Description	Number
94(1a)(a)	The total number of requests made under Division 3 of Part III to issuing authorities during the year for the issue of warrants under that division	0
94(1A)(b)	The total number of warrants issued during the year under that division	0
94(1A)(c)	The total number of warrants issued during the year under section 34E	0
94(1A)(d)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year under section 34E and the total of all those hours for all those persons	0
94(1A)(e)	The total number of warrants issued during the year under section 34G	0
94(A)(f)(i)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year under section 34G	0
94(A)(f)(ii)	The number of hours each person spent in detention under such a warrant	0
94(A)(f)(iii)	The total of all those hours for all those persons	0
94(1A)(g)	The number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	0

# Appendix D

## Workforce statistics

**Table 1: Composition of workforce 2007–08 to 2012–13<sup>1</sup>**

(Does not include the Director-General)

	2007–08	2008–09	2009–10	2010–11	2011–12	2012–13
Ongoing full-time	1,263	1,452	1,460	1,511	1,546	1,589
Non-ongoing full-time	52	49	40	50	37	42
Ongoing part time	108	116	134	148	168	193
Non-ongoing part-time	12	19	18	16	18	19
Non-ongoing casual	57	54	39	42	43	61
<b>Total</b>	<b>1,492</b>	<b>1,690</b>	<b>1,691</b>	<b>1,767</b>	<b>1,812</b>	<b>1,904</b>

<sup>1</sup> Includes secondees and locally engaged staff held against positions in the structure

**Table 2: Senior Executive Service (SES) equivalent classification and gender 2007–08 to 2012–13**

(Does not include the Director-General)

		2007–08	2008–09	2009–10	2010–11	2011–12	2012–13
Band 1	Female	6	7	6	8	10	8
	Male	29	35	35	38	36	27
Band 2	Female	2	4	4	4	5	3
	Male	11	12	10	10	8	6
Band 3	Female	0	0	0	0	0 <sup>1</sup>	0 <sup>1</sup>
	Male	2	2	2	2	1	1
<b>Total</b>		<b>50</b>	<b>60</b>	<b>57</b>	<b>62</b>	<b>60</b>	<b>45</b>

<sup>1</sup> These figures do not include a seconded Band 3.

**Table 3: Representation of designated groups within ASIO at 30 June 2013**

(Does not include the Director-General)

Group	Total staff <sup>1</sup>	Women	Non-English speaking background	Aboriginal and Torres Strait Islander	People with a disability	Available EEO Data <sup>2</sup>
SES	45	11	0	0	1	43
Senior Officers <sup>3</sup>	517	185	19	2	9	476
AO5 <sup>4</sup>	641	331	48	3	7	580
AO1-4 <sup>5</sup>	591	292	29	3	3	557
Information Technology Officers Grades 1 and 2	102	15	6	0	3	97
Engineers Grades 1 and 2	8	0	0	0	0	8
<b>Total</b>	<b>1,904</b>	<b>834</b>	<b>102</b>	<b>8</b>	<b>23</b>	<b>1,761</b>

<sup>1</sup> Based on staff salary classifications recorded in ASIO's human resource information system

<sup>2</sup> Provision of EEO data is voluntary

<sup>3</sup> Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications

<sup>4</sup> ASIO Officer grade 5 group translates to APS Level 6

<sup>5</sup> Translates to span the APS 1 to 5 classification levels

**Table 4: Percentage of representation of designated groups in ASIO 2007-08 to 2012-13**

Group	2007-08	2008-09	2009-10	2010-11	2011-12	2012-13
Women <sup>1</sup>	45.4	44.6	44.3	44.3	44.3	<b>43.8</b>
Non-English speaking background	4.4	5.6	6.9	6.0	5.7	<b>5.8</b>
Aboriginal Torres Strait Islander	0.3	0.2	0.2	0.3	0.4	<b>0.5</b>
People with a disability	1.4	1.4	1.2	1.2	1.2	<b>1.3</b>

<sup>1</sup> Percentages for women are based on total staff. Percentages for other groups are based on staff for whom EEO data was available

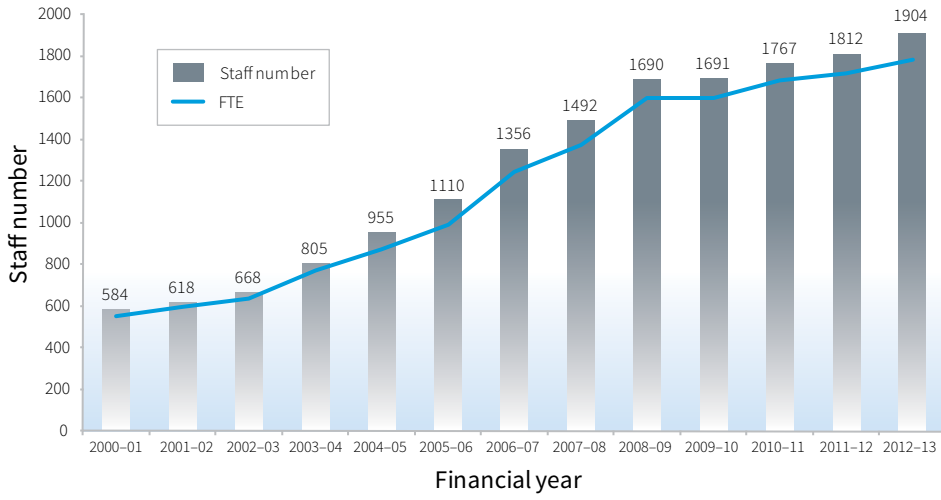


# Appendix E

## ASIO salary classification structure at 30 June 2013

ASIO MANAGERS			
SES Band 3	\$232,491		minimum point
SES Band 2	\$208,888		minimum point
SES Band 1	\$170,683		minimum point
AE03	\$124,131		
AE02	\$112,611	to	\$124,131
AE01	\$99,297	to	\$112,611
INTELLIGENCE OFFICERS			
IO	\$75,821	to	\$86,484
ASIO OFFICERS			
ASIO Officer 5	\$75,821	to	\$86,484
ASIO Officer 4	\$62,533	to	\$70,288
ASIO Officer 3	\$54,532	to	\$60,240
ASIO Officer 2	\$48,022	to	\$53,121
ASIO Officer 1	\$42,565	to	\$46,921
ASIO Information Technology Officers			
SITOA	\$124,131		
SITOB	\$112,611	to	\$124,131
SITOC	\$99,297	to	\$107,183
ITO2	\$75,821	to	\$86,484
ITO1	\$58,759	to	\$68,261
ASIO ENGINEERS			
SIO(E)5	\$126,103		
SIO(E)4	\$112,611	to	\$124,131
SIO(E)3	\$99,297	to	\$107,183
SIO(E)2	\$75,821	to	\$86,484
SIO(E)1	\$58,759	to	\$68,261

## ASIO staff numbers 2001-13



# Compliance Index

Part of report	Description	Requirement	Page
	Letter of transmittal	Mandatory	iii
	Table of contents	Mandatory	v,vi
	Index	Mandatory	131
	Glossary	Mandatory	129–130
	Contact officer(s)	Mandatory	Back cover
	Internet home page address and Internet address for report	Mandatory	Back cover
<b>Review by secretary [or equivalent]</b>			
	Review by departmental secretary [or equivalent]	Mandatory	vii–ix
	Summary of significant issues and developments	Suggested	vii–ix
	Overview of department's performance and financial results	Suggested	ix
	Outlook for following year	Suggested	Part 1
	Significant issues and developments – portfolio	Portfolio departments – suggested	Not applicable
<b>Departmental overview</b>			
	Role and functions	Mandatory	xii
	Organisational structure	Mandatory	xiii–xiv
	Outcome and program structure	Mandatory	x, 10
	Where outcome and program structures differ from PB Statements/PAES or other portfolio statements accompanying any other additional appropriation bills (other portfolio statements), details of variation and reasons for change	Mandatory	Not applicable
	Portfolio structure	Portfolio departments – Mandatory	Not applicable
<b>Report on performance</b>			
	Review of performance during the year in relation to programs and contributions to outcomes	Mandatory	Part 2
	Actual performance in relation to deliverables and Key Performance Indicators set out in Portfolio Budget Statements/Portfolio Additional Estimates Statements or other portfolio statements	Mandatory	Part 2

Part of report	Description	Requirement	Page
	Where performance targets differ from the PBS/PAES, details of both former and new targets, and reasons for the change	Mandatory	Not applicable
	Narrative discussion and analysis of performance	Mandatory	Part 2
	Trend information	Mandatory	Throughout
	Significant changes in nature of principal functions/services	Suggested	Not applicable
	Performance of purchaser/provider arrangements	If applicable, suggested	Not applicable
	Factors, events or trends influencing departmental performance	Suggested	Part 1
	Contribution of risk management in achieving objectives	Suggested	52
	Social inclusion outcomes	If applicable, mandatory	Not applicable
	Performance against service charter-customer service standards, complaints data, and the department's response to complaints	If applicable, mandatory	38, 47, 59–60
	Discussion and analysis of the department's financial performance	Mandatory	Part 6
	Discussion of any significant changes from the prior year, from budget or anticipated to have a significant impact on future operations	Mandatory	ix
	Agency resource statement and summary resource tables by outcomes	Mandatory	116

## Management and accountability

### Corporate governance

	Agency heads are required to certify that their agency complies with the Commonwealth Fraud Control Guidelines	Mandatory	iii
	Statement of the main corporate governance practices in place	Mandatory	50–52
	Names of the senior executive and their responsibilities	Suggested	–
	Senior management committees and their roles	Suggested	50–52
	Corporate and operational planning and associated performance reporting and review	Suggested	52

Part of report	Description	Requirement	Page
	Approach adopted to identifying areas of significant financial or operational risk	Suggested	52
	Policy and practices on the establishment and maintenance of appropriate ethical standards	Suggested	
	How nature and amount of remuneration for SES officers is determined	Suggested	103
<b>External scrutiny</b>			
	Significant developments in external scrutiny	Mandatory	36–40
	Judicial decisions and decisions of administrative tribunals	Mandatory	19–21
	Reports by the Auditor-General, a Parliamentary Committee or the Commonwealth Ombudsman	Mandatory	Not applicable
<b>Management of human resources</b>			
	Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	53–59
	Workforce planning, staff turnover and retention	Suggested	53–56
	Impact and features of enterprise or collective agreements, individual flexibility arrangements (IFAs), determinations, common-law contracts and AWAs	Suggested	59
	Training and development undertaken and its impact	Suggested	56, 58
	Work health and safety performance	Suggested	60–61
	Productivity gains	Suggested	–
	Statistics on staffing	Mandatory	119–122
	Enterprise or collective agreements, IFAs, determinations, common-law contracts and AWAs	Mandatory	59
	Performance pay	Mandatory	Not applicable
	Assessment of effectiveness of assets management	If applicable, mandatory	64
	Assessment of purchasing against core policies and principles	Mandatory	64

Part of report	Description	Requirement	Page
	The annual report must include a summary statement detailing the number of new consultancy services contracts let during the year; the total actual expenditure on all new consultancy contracts let during the year (inclusive of GST); the number of ongoing consultancy contracts that were active in the reporting year; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST). The annual report must include a statement noting that information on contracts and consultancies is available through the AusTender website.	Mandatory	64
	Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	Not applicable
	Contracts exempt from the AusTender	Mandatory	64
	Financial statements	Mandatory	Part 6
<b>Other Mandatory Information</b>			
	Work health and safety (Schedule 2, Part 4 of the <i>Work Health and Safety Act 2011</i> )	Mandatory	60–61
	Advertising and market research (section 311A of the <i>Commonwealth Electoral Act 1918</i> ) and statement on advertising campaigns	Mandatory	56
	Ecologically sustainable development and environmental performance (Section 516A of the <i>Environment Protection and Biodiversity Conservation Act 1999</i> )	Mandatory	62–63
	Compliance with the agency's obligations under the <i>Carer Recognition Act 2010</i>	If applicable, mandatory	Not applicable
	Grant programs	Mandatory	Not applicable
	Disability reporting—explicit and transparent reference to agency-level information available through other reporting mechanisms	Mandatory	120
	Information Publication Scheme statement	Mandatory	Not applicable

Part of report	Description	Requirement	Page
	Spatial reporting—expenditure by program between regional and non-regional Australia	If applicable, mandatory	64
	Correction of material errors in previous annual report	If applicable, mandatory	Not applicable
	Agency resource statements and resources for outcomes	Mandatory	116
	List of requirements	Mandatory	Appendix

## Additional ASIO reporting requirements (under the ASIO Act)

Part of report	Description	Requirement	Page
	The total number of requests made under Division 3 of Part III to issuing authorities during the year for the issue of warrants under that Division	Mandatory	Part 3
	The total warrants issued during the year under that Division	Mandatory	Part 3
	The total number of warrants issued during the year under section 34E and the total of all those hours for all those persons	Mandatory	Part 3
	The following numbers: <ul style="list-style-type: none"> <li>▶ The number of hours each person appeared before a prescribed authority for questions under warrant issued during the year under section 34G</li> <li>▶ The number of hours each person spent in detention under such a warrant</li> <li>▶ The total of all those hours for all those persons</li> </ul>	Mandatory	Part 3
	The number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	Mandatory	Part 3



# Glossary

---

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
ANU	Australian National University
ANZCTC	Australia and New Zealand Counter-Terrorism Committee
AQAP	Al-Qa'ida in the Arabian Peninsula
ASD	Australian Signals Directorate
ASIC	Aviation Security Identification Card
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
BLU	Business Liaison Unit
CERT Australia	Computer Emergency Response Team Australia
COAG	Council of Australian Governments
CRS	Contact Reporting Scheme
CTCC	Counter Terrorism Control Centre
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DIS	Defence Intelligence Security
EMS	Environmental Management System
FOI Act	<i>Freedom of Information Act 1982</i>
G20	Group of Twenty
GST	goods and services tax
IDP	Intelligence Development Program
IGIS	Inspector-General of Intelligence and Security
INSLM	Independent National Security Legislation Monitor
ISA	<i>Intelligence Services Act 2001</i>
IT	information technology
MSIC	Maritime Security Identification Card
NAA	National Archives of Australia
NiTAC	National Interception Technical Assistance Centre
NSW CCA	New South Wales Criminal Court of Appeal
NTAC	National Threat Assessment Centre
PGPA Act	<i>Performance and Accountability Act 2013</i>
PID Act	<i>Public Interest Disclosure Act 2013</i>

PJCIS	Parliamentary Joint Committee on Intelligence and Security
PMC	Department of the Prime Minister and Cabinet
PSPF	Protective Security Policy Framework
PSRR	Protective Security Risk Review
SCEC	Security Construction and Equipment Committee
SEEPL	Security Equipment Evaluated Product List
SSAN	security-sensitive ammonium nitrates
SSBA	security-sensitive biological agents
WHS	work health and safety
WHS Act	<i>Work Health and Safety Act 2011</i>

# Index

---

## A

accountability ix, xi, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 50, 51, 53

Administrative Appeals Tribunal (AAT) 16, 20, 21, 41, 67

adverse security assessments 15, 16, 17, 18, 19, 20, 21, 39, 40. *See also* security assessments

Afghanistan 4, 12

Africa 4

al-Qa'ida viii, x, 3, 4, 12, 14

al-Qa'ida in the Arabian Peninsula (AQAP) 3, 4, 14

Algeria 4

Arab Spring 2, 4, 13

*Archives Act 1983* 66

ASIO Security Committee 52

assessments

- strategic 10, 11, 12
- threat 7, 10, 11, 12, 13, 27
- visa security x, 15, 17, 18

assets 13, 23, 62, 75, 76, 77, 81, 83, 84, 85, 86, 87, 88, 89, 90, 91, 93, 94, 95, 99, 101, 102, 106, 107, 108, 109, 111

assumed identities 44

asylum seekers 18, 38

Attorney-General xi, xii, 14, 15, 22, 29, 36, 37, 41

Attorney-General's Department 12, 14, 18, 24, 37, 56

Attorney-General's Guidelines 36

audit xi, 43, 44, 46, 52, 53, 60, 102

Audit and Risk Committee 43, 52, 53

AusCheck 18

Australia vii, viii, ix, x, xi, xii, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14, 15, 16, 17, 22, 23, 25, 26, 27, 28, 29, 37, 38, 40, 42, 46, 47, 48, 49, 54, 59, 63, 65, 69, 83, 115, 117

*Australia and New Zealand Counter-Terrorism Committee (ANZCTC)* 28

*Australian Citizenship Act 2007* 17

Australian Cyber Security Centre 62

Australian Federal Police (AFP) 12, 18, 26, 28, 56

Australian Geospatial-Intelligence Organisation (AGO) 56. *See also* Defence Imagery and Geospatial Organisation (DIGO)

Australian Government x, 5, 6, 10, 11, 12, 13, 14, 16, 18, 19, 22, 23, 24, 27, 28, 36, 45, 48, 52, 65, 67, 75, 77, 89, 86, 91, 112

Australian Government Security Vetting Agency (AGSVA) 19

Australian Government Solicitor 14

Australian Intelligence Community xii, 5, 12, 14, 26, 36, 37, 38, 42, 47

Australian National Audit Office (ANAO) 44

Australian National University, The (ANU) 48, 57

Australian Nuclear Science and Technology Organisation (ANSTO) 18

*Australian Passports Act 2005* 16

Australian Secret Intelligence Service (ASIS) 12, 26, 29, 56

*Australian Security Intelligence Organisation Act 1979* (ASIO Act) ix, xi, xii, 7, 15, 17, 22, 29, 36, 37, 83, 118

Australian Signals Directorate (ASD) 12, 13, 26, 29, 56. *See also* Defence Signals Directorate (DSD)

Aviation Security Identification Card (ASIC) 18

## B

Bali bombing 13

border integrity xii, 2, 8, 25, 27, 28

border security 10, 17. *See also* people smuggling

*Border Security Legislation Amendment Act 2002* 36

*Boston Marathon bombing* vii, 2, 13

Business Liaison Unit (BLU) 14, 47

## C

Career and Talent Management Framework 55  
Code of Conduct 58, 60, 61  
Comcare 61, 62  
*Commonwealth Crimes Act 1914* 44  
Commonwealth Director of Public Prosecutions 20, 28  
Commonwealth Procurement Rules 65  
communal violence viii, x, xii, 2, 3, 7, 8, 12  
complaints 38, 47, 61  
Consolidated Determination 59  
consultants 24, 65  
Contact Reporting Scheme 27  
Corporate Committee Framework 50  
corporate governance x, 43, 50, 52, 53  
Council of Australian Governments (COAG) 18, 42  
counter-espionage 11, 25, 26, 27, 115. *See also* espionage  
counter-terrorism x, 4, 10, 11, 18, 25, 26, 28, 40, 42, 69, 115. *See also* terrorism  
Counter Intelligence and Security Review Committee 52  
Counter Terrorism Control Centre (CTCC) 26  
*Criminal Code Act 1995* (Criminal Code) 14, 20, 37  
*Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* 36  
critical infrastructure viii, 4, 7, 10, 12, 13, 23, 28, 37, 49  
cyber espionage 5, 13. *See also* cyber security; *See also* espionage  
cyber security 13, 38. *See also* cyber espionage; *See also* espionage

## D

Defence Imagery and Geospatial Organisation (DIGO) 56.  
*See also* Australian Geospatial-Intelligence Organisation (AGO)  
Defence Intelligence Organisation (DIO) 12

Defence Intelligence Security (DIS) 23  
Defence Signals Directorate (DSD) 12, 56. *See also* Australian Signals Directorate (ASD)  
Department of Defence 19, 23, 26  
Department of Finance and Deregulation 62, 86, 91, 112  
Department of Foreign Affairs and Trade (DFAT) 12, 13, 14, 21, 56, 112  
Department of Human Services 56  
Department of Infrastructure and Transport 12, 56  
Department of the Prime Minister and Cabinet (PMC) 12, 55, 67, 116  
Department of the Treasury 56  
Deputy Director-General, Capability and Assessments Coordination 37  
Director-General of Security vii, ix, xi, xv, 9, 19, 20, 21, 31, 36, 37, 39, 40, 43, 46, 48, 49, 51, 52, 53, 61, 69, 71, 84, 91, 115, 119, 120

## E

e-learning 59, 61  
Egypt 13, 38  
engagement ix, 6, 11, 13, 14, 25, 41, 47, 48, 62, 67  
environmental performance 63, 64  
espionage viii, x, xii, 2, 5, 6, 11, 12, 13, 22, 26, 27, 31, 115. *See also* cyber espionage; *See also* cyber security  
Executive Board 51, 52, 53, 60  
Expert Panel on Asylum Seekers 18. *See also* Houston Review  
extremism vii, 2, 12

## F

Federal Court of Australia 16, 20, 21, 41  
Finance Committee 52  
*Financial Management and Accountability Act 1997* (FMA Act) 43, 71, 83, 112

*Financial Management and Accountability Regulations* 43  
financial statements xii, 36, 44, 69, 71, 83, 84, 86, 91  
foreign intelligence x, xii, 6, 10, 20, 27, 29  
foreign interference viii, x, xii, 2, 6, 7, 12, 20, 22, 25, 26, 27  
fraud 43, 44, 52  
*Freedom of Information Act 1982* (FOI Act) 66

## G

G20 8, 13, 18, 28

## H

High Court of Australia 16, 19, 20, 41, 91  
Horner AM, Professor David 48  
Houston Review 18. *See also* Expert Panel on Asylum Seekers  
Human Capital Framework 54, 55

## I

Independent National Security Legislation Monitor (INSLM) 40, 41  
Independent Reviewer of Adverse Security Assessments 16, 20, 39, 40, 41  
information and communications technology 3, 46, 56, 67  
information technology (IT) x, 46, 52, 56, 57, 120, 121  
*Innocence of Muslims* 8  
  
Inspector-General of Intelligence and Security (IGIS) 16, 38, 44, 66, 67  
*Inspire magazine* 3  
Intelligence Coordination Committee 50  
Intelligence Development Program (IDP) 59  
*Intelligence Services Act 2001* (the ISA) ix, 36, 37  
Inter Agency Security Forum 24  
international partners viii, xii, 13, 25, 28, 51, 67

## J

Jabhat al-Nusra 3, 12, 15  
Job Family Model 55

## K

Khazaal, Belal 20

## L

Lebanon 3  
legislative reviews/reforms ix, 37, 40, 41, 42  
litigation 11, 19  
London Olympic and Paralympic Games 13  
lone actor vii, 2, 12, 13

## M

Management and Leadership in Security Intelligence strategy x, 58  
Maritime Security Identification Card (MSIC) 18  
Middle East 2, 3, 4  
Minister for Defence xii, 10, 29  
Minister for Foreign Affairs xii, 10, 21, 29  
Minister for Immigration and Citizenship 17, 20, 21

## N

National Archives of Australia (NAA) 48, 66, 67  
National Counter-Terrorism Plan 28  
National Intelligence Priorities 28  
National Interception Technical Assistance Centre (NiTAC) 59  
national security ix, xi, 5, 11, 14, 15, 16, 18, 19, 23, 25, 27, 28, 29, 33, 36, 37, 38, 40, 42, 47, 48, 51, 65, 66, 83  
National Security Committee of Cabinet 29  
national security community 11, 26, 47, 67  
*National Security Information (Criminal and Civil Proceedings) Act 2004* 40

National Threat Assessment Centre (NTAC)  
12, 13  
new ASIO building 52, 63, 79, 112. *See also*  
new central office  
New Building Committee 52  
new central office 53, 63. *See also* new ASIO  
building  
New South Wales Court of Criminal Appeal  
20  
New South Wales Police Force 12, 56  
North Africa 4  
*NSW Law Enforcement and National Security*  
*(Assumed Identities) Act 2010* 44  
*New South Wales Minister for Police and*  
*Emergency Services* 44

## O

Office of National Assessments (ONA) 12, 56  
Office of Transport Security 56  
official history of ASIO 48  
Ombudsman 60, 61  
Organisational Capability Program 57  
outreach 46, 56

## P

Pakistan 4  
Parliamentary Joint Committee on  
Intelligence and Security (PJCIS) ix,  
36, 37, 65, 66  
PJCIS review of national security legislation  
ix, 36, 37  
passports 15, 16, 21  
people smuggling x, 8, 12, 27.  
*See also* border security  
politically motivated violence xii, 2, 21  
proscription 3, 11, 14, 15, 37  
protective security xii, 6, 10, 12, 13, 18, 22,  
23, 24, 45, 52  
Protective Security Policy Committee 24  
Protective Security Policy Framework  
(PSPF) 18, 22, 24, 27, 45  
protective security risk reviews (PSRR) 23

Protective Security Training Centre 24  
protest activity 7, 8, 12, 13  
*Public Interest Disclosure Act 2013* 42

## Q

Queensland Police Service 56  
questioning and detention warrants 36, 118

## R

records 38, 41, 44, 66, 67, 71  
recruitment 27, 54, 55, 56, 57  
reviews xi, 16, 19, 22, 23, 36, 37, 38, 39, 40, 41,  
42, 44, 45, 46, 50, 52, 53, 55, 59, 60,  
61, 65, 79, 85, 90  
risk viii, ix, 8, 10, 12, 14, 17, 22, 23, 37, 41, 42,  
44, 46, 47, 48, 51, 52, 53, 54, 61, 62,  
84, 87, 91, 108, 109  
risk management 14, 47, 52, 53, 61

## S

security assessments  
adverse 15, 16, 17, 18, 19, 20, 21, 39, 40  
advice 11, 15, 18, 19  
appeal mechanisms 16  
counter-terrorism x, 10, 18  
personnel x, 10, 18, 19  
qualified 15, 16, 18, 40  
visa x, 15, 17, 18  
Security Construction and Equipment  
Committee (SCEC) 24  
security environment vii, x, xi, 1, 11, 12, 25,  
35, 36, 37, 47, 51, 58  
Security Equipment Evaluated Product List  
(SEEPL) 24  
*Security Legislation Amendment (Terrorism)*  
*Act 2002* 36  
security-sensitive ammonium nitrates  
(SSAN) 18  
security-sensitive biological agents (SSBA)  
18  
Senate Estimates ix, 37

Senior Executive Service xii, 47, 48, 52, 55, 64, 91, 103, 119  
Somalia 4  
South Asia 4  
South-East Asia 4, 12  
Staff and Family Liaison Office 62  
staffing and resource allocation review 55  
Stakeholder Satisfaction Survey 10, 47  
Strategic Plan 2013–16 x, 50, 51  
Strategic Risk Management Framework 53  
Strategic Workforce Plan 54  
*Suppression of the Financing of Terrorism Act 2002* 36  
Syria viii, x, 2, 3, 7, 12, 13

## T

T4 22, 23, 24  
technical capabilities x, 5, 26, 54, 56  
technical surveillance countermeasures 22, 23  
*Telecommunications (Interception and Access) Act 1979* ix, 37  
terrorism vii, x, 2, 3, 4, 11, 12, 13, 15, 16, 18, 19, 20, 22, 25, 28, 40, 42. *See also* counter-terrorism  
terrorist groups/organisations viii, 3, 12, 37  
threat assessments 7, 10, 11, 12, 13, 27.  
*See also* assessments  
Top Secret certification 22, 23  
trusted insider viii, x

## U

unauthorised maritime arrivals 8, 12, 17, 19, 20, 21, 38  
United Kingdom vii, 2  
United States of America vii

## V

vetting 19, 54, 56  
Victoria Police 56  
violent protest 7, 8, 12

visa security assessments x, 15, 17, 18.  
*See also* assessments

## W

Walker SC, Bret 40  
warrants xii, 36, 41, 118  
Western Australia Police 56  
whole-of-government 8, 27, 42, 45, 48  
Woolwich attack vii, 13  
*Work Health and Safety Act 2012* (WHS Act) 44, 60, 61, 62  
work health and safety (WHS) 44, 52, 60, 61, 62  
Work Health and Safety Committee 52  
Workforce Capability Committee 50  
workforce planning x, 54, 55, 56  
workplace agreement 60

## Y

Yemen 4





## Contact and internet details

### Written inquiries

The Director-General of Security  
ASIO Central Office  
GPO Box 2176  
CANBERRA ACT 2601

### General inquiries

Central Office switchboard  
Tel: (02) 6249 6299  
1800 020 648 (toll free)  
Fax: (02) 6257 4501

### Media inquiries

Media Liaison Officer  
Tel: (02) 6249 8381  
Fax: (02) 6262 9547

### Website

[www.asio.gov.au](http://www.asio.gov.au)

---

## Report a threat

### National Security Hotline

Tel: 1800 123 400  
Email: [hotline@nationalsecurity.gov.au](mailto:hotline@nationalsecurity.gov.au)

---

## State and territory offices

Australian Capital Territory	(02) 6249 6299
Victoria	(03) 9654 8985
New South Wales	(02) 8904 0251
Queensland	(07) 3831 5980
South Australia	(08) 8223 2727
Western Australia	(08) 9221 5066
Tasmania	1800 020 648
Northern Territory	(08) 8981 2374

---

## Supplementary information

The ASIO Strategic Plan 2013–16 provides further information on the activities and management of ASIO, and is available on the ASIO website.

---

