



Australian Government

Australian Security  
Intelligence Organisation

# ASIO Annual Report 2019–20



Securing Australia—protecting its people

# Aids to access

© Commonwealth of Australia 2020

ISSN 0815–4562 (print)

ISSN 2204–4213 (online)

## Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

## Creative Commons licence

With the exception of the Coat of Arms, this publication is licensed under a Creative Commons Attribution 3.0 Australia Licence.



Creative Commons Attribution 3.0 Australia Licence is a standard form licence agreement that allows you to copy, distribute, transmit and adapt this publication provided that you attribute the work. A summary of the licence terms is available from <http://creativecommons.org/licenses/by/3.0/au/deed.en>. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.

The Commonwealth's preference is that you attribute this publication (and any material sourced from it) using the following wording:

**Source:** Licensed from the Commonwealth of Australia under a Creative Commons Attribution 3.0 Australia Licence. The Commonwealth of Australia does not necessarily endorse the content of this publication.

## Commonwealth Coat of Arms

The Commonwealth Coat of Arms is used in accord with the April 2014 *Commonwealth Coat of Arms: information and guidelines*, published by the Department of the Prime Minister and Cabinet and available online ([http://www.pmc.gov.au/sites/default/files/publications/Commonwealth\\_Coat\\_of\\_Arms\\_Information\\_and\\_Guidelines.pdf](http://www.pmc.gov.au/sites/default/files/publications/Commonwealth_Coat_of_Arms_Information_and_Guidelines.pdf)).

## Report a threat

National Security Hotline 1800 123 400  
[hotline@nationalecurity.gov.au](mailto:hotline@nationalecurity.gov.au)

## About this report

This report has been prepared in accordance with the provisions of the *Public Governance Performance and Accountability Act 2013* (PGPA Act), the Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) and the Department of Finance Resource Management Guide Number 135.

## Location of this annual report

Further information about ASIO and an online version of this report are available on the ASIO website. The direct address to view this annual report is [www.asio.gov.au/asio-report-parliament](http://www.asio.gov.au/asio-report-parliament). The annual report can also be viewed at [www.transparency.gov.au](http://www.transparency.gov.au).

## Contact us

We welcome feedback on our annual report from any of our readers.

### Phone

General inquiries	1800 020 648
ASIO Outreach inquiries	02 6234 1688
Media inquiries	02 6249 8381
Recruitment inquiries	02 6257 4916

### Email

[media@asio.gov.au](mailto:media@asio.gov.au)

### Post

GPO Box 2176, Canberra ACT 2601

### State and territory offices

Call 13ASIO (132746)

## Acknowledgement of Country

ASIO acknowledges the traditional owners and custodians of country throughout Australia, and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, the cultures and elders past, present and emerging. We also acknowledge the contributions of our Aboriginal and Torres Strait Islander employees in support of our mission.

## Photographs

Since 2014, ASIO has held an annual photography competition inviting staff to submit images to include in the annual report. The most popular image chosen through an all-staff poll appears as a chapter page.



---

# **ASIO Annual Report 2019–20**



21<sup>st</sup> September 2020  
Ref: A18535815

The Hon. Peter Dutton MP  
Minister for Home Affairs  
Parliament House  
CANBERRA ACT 2600

Dear Minister,

ASIO Annual Report 2019-20

In accordance with section 46 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), I am pleased to present to you the Australian Security Intelligence Organisation's (ASIO) annual report for 2019-20.

This report contains information required by the PGPA Rule 2014 and section 94 of the Australian Security Intelligence Organisation Act 1979 (ASIO Act). In order to ensure compliance with the Determination made by the Minister for Finance under section 105D of the PGPA Act, the statements required under subsection 94(2A) of the ASIO Act relating to special intelligence operations and telecommunications data authorisations have been removed from the annual report tabled in the Parliament in order to avoid prejudice to ASIO's activities. These statements will be separately provided to you and, as required by the ASIO Act, to the Leader of the Opposition. The statement relating to telecommunications data authorisations will also be provided to the Parliamentary Joint Committee on Intelligence and Security.

As required by subsection 17AG(2) of the PGPA Rule, I certify that fraud risk assessments and control plans have been prepared for ASIO, that we have appropriate mechanisms in place for preventing, investigating, detecting and reporting incidents of fraud, and that all reasonable measures have been taken to deal appropriately with fraud.

Yours sincerely,

Mike Burgess

---

# At a glance

p. 2

## Director-General's review

The threats of terrorism, espionage and foreign interference recognise no borders. They are persistent, and their enduring nature means we cannot afford to rest on our successes.

p. 9

## Commitment to legality and propriety

ASIO must operate lawfully, in proportion to the threats we are investigating, and in line with the standards and expectations of the Australian community. We don't just do what is legal, we do what is right.

p. 10

## Out-thinking Australia's adversaries

We need people who can out-think and out-imagine our adversaries to achieve our mission of protecting Australia and Australians. We also need to ensure that our workforce continues to mirror the diversity of the society we serve.

p. 12

### Organisational chart

ASIO's new organisational structure sets out clear lines of authority and responsibility.

p. 17

### Terrorism threat

Australia's national terrorism threat level remains at **PROBABLE**. The primary threat remains Sunni Islamic extremism, but other violent ideologies—such as those of the extreme right—are also of concern.

p. 23

### Counter-espionage and foreign interference

The threat to Australia from foreign states seeking to obtain strategic advantage at the expense of Australia and its interests cannot be understated.

p. 59

### ASIO's response to COVID-19

In response to COVID-19, ASIO adapted its operating model to maintain coverage of high-priority targets related to our counter-terrorism and counter-espionage and foreign interference missions.

p. 63

### Compliance

Ethical behaviour and integrity are core values of the Organisation.

# Contents

<b>1</b>	<b>Director-General's review</b>	<b>1</b>
<b>2</b>	<b>Overview of ASIO</b>	<b>7</b>
<b>3</b>	<b>Australia's security environment and outlook</b>	<b>15</b>
<b>4</b>	<b>Report on performance</b>	<b>27</b>
	Annual performance statement 2019–20	29
	ASIO's purpose	30
	Results for 2019–20	31
	<b>Key mission 1:</b> counter-terrorism	32
	<b>Key mission 2:</b> counter-espionage and foreign interference	39
	<b>Key mission 3:</b> border integrity, including people smuggling	45
	<b>Key mission 4:</b> protective security advice	50
	Analysis of performance	53
	Report on financial performance	54
<b>5</b>	<b>Management and accountability</b>	<b>55</b>
	Corporate governance	57
	ASIO's response to COVID-19	59
	External scrutiny	60
	Compliance	63
	Significant legal matters affecting ASIO's business	65
	Management of human resources	67
	Other mandatory information	71
	Information required by another Act or instrument	72



<b>F</b>	<b>Financial statements</b>	<b>75</b>
<b>A</b>	<b>Appendices</b>	<b>109</b>
	Appendix A: ASIO resource statement	111
	Appendix B: expenses by outcomes	112
	Appendix C: executive remuneration	113
	Appendix D: ASIO's salary classification structure	117
	Appendix E: workforce statistics by headcount	118
	Appendix F: work health and safety	122
	Appendix G: recruitment, advertising and market research	124
	Appendix H: ecologically sustainable development and environmental performance	125
	Appendix I: report of the Independent Reviewer of Adverse Security Assessments	128
	Appendix J: report on use of questioning warrants and questioning and detention warrants	130
	List of annual report requirements under schedule 2 of the Public Governance, Performance and Accountability Rule	131
	List of annual report requirements under other legislation	138
	Abbreviations and short forms	139
	Glossary	142
	Index	144



Securing Australia—protecting its people



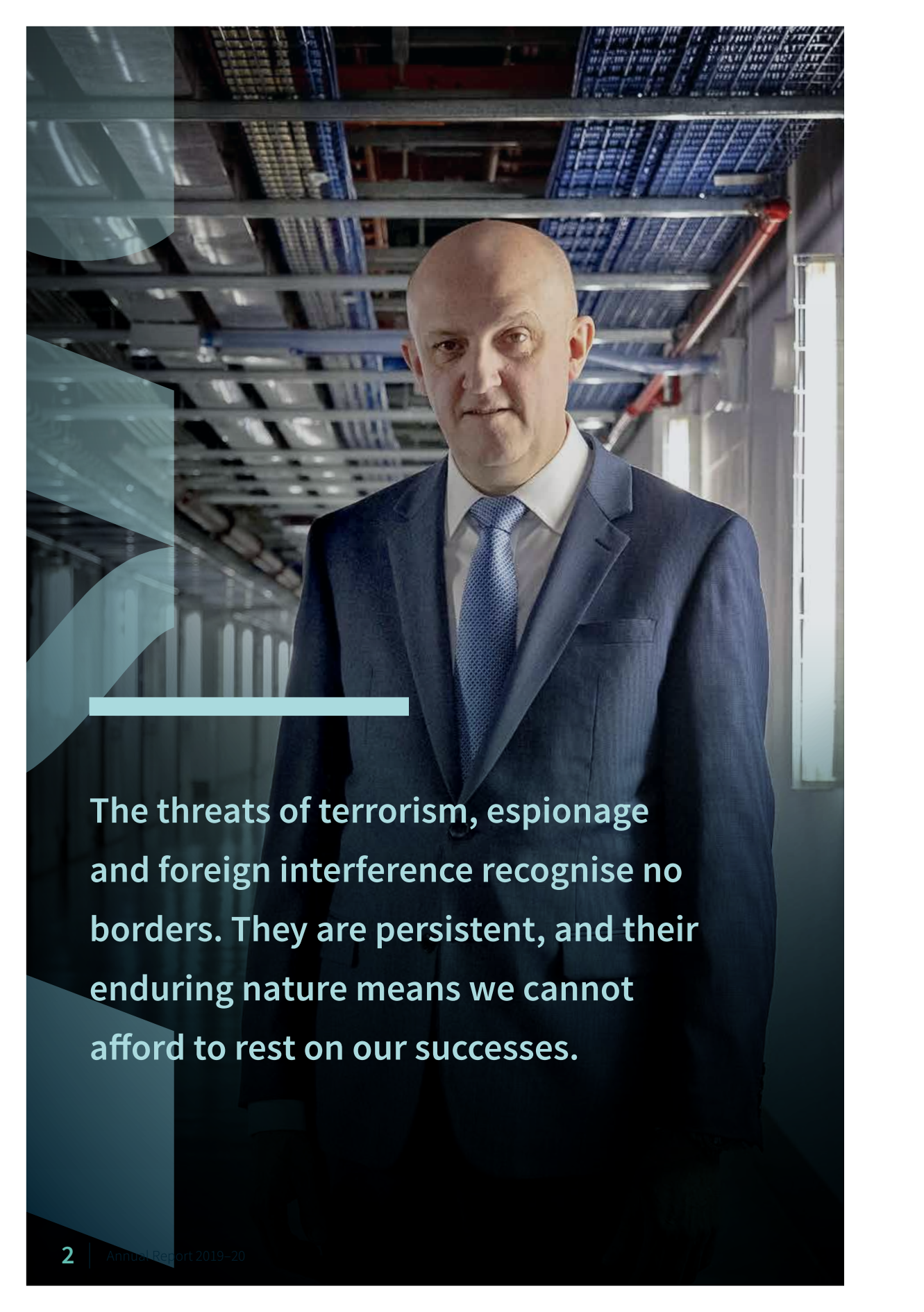


A low-angle, upward-looking photograph of a dense forest. The image shows the intricate network of dark tree trunks and branches reaching towards a bright, clear blue sky. The perspective creates a sense of height and grandeur. The foliage is lush and green, filling the upper portions of the frame.

# 1

**Director-General's  
review**





The threats of terrorism, espionage and foreign interference recognise no borders. They are persistent, and their enduring nature means we cannot afford to rest on our successes.

# Director-General's review

## Introduction

The view from the Director-General's office is dominated by two buildings—Parliament House and the High Court.

To me, they are concrete reminders that Parliament grants ASIO extraordinary powers, but those powers must always be exercised legally and ethically, with rigorous oversight.

This is something I reflect on every day. When I am approached to apply for a warrant so we can track a potential terrorist, approve an investigation into a suspected spy or consider security advice that might result in a visa cancellation, I ask:

- Are our proposed activities proportionate to the threat?
- Are we using the least intrusive methods possible?
- Are we acting within the letter and the spirit of the law?

In 2019–20 an evolving security environment forced ASIO to use its powers on multiple occasions. Not even a global pandemic could curtail the threats facing Australia. In some cases, it amplified them.

## Threat environment

Australia's threat environment is complex, challenging and changing.

The terrorism threat level remains at **PROBABLE**, and I see no prospect it will be lowered in the foreseeable future. Sunni Islamic extremism remains ASIO's greatest concern.

We know that:

- Groups such as Islamic State of Iraq and the Levant (ISIL) continue to call on their supporters to conduct terrorist attacks, with Australia specifically identified as a target.
- Around 80 Australians who travelled to Syria and Iraq to fight for or support Islamic extremist groups are still in the region, and some may bring extremist ideology back to Australia.
- Individuals in Australia continue to be radicalised, and the online amplification of radicalisation messages is reaching ever-younger targets.
- Multiple terrorism offenders are scheduled for release from Australian prisons over the next five years.

At the same time, right-wing extremists are more organised, sophisticated, ideological and active than previous years.

While we have been actively monitoring the threat for some time, this year extreme right-wing individuals comprised around one-third of our counter-terrorism investigative subjects.

Many of these groups and individuals have seized on COVID-19, believing it reinforces the narratives and conspiracies at the core of their ideologies. They see the pandemic as proof of the failure of globalisation, multiculturalism and democracy, and confirmation that societal collapse and a 'race war' are inevitable.

## Foreign interference

While terrorism is a threat to life, espionage and foreign interference represent threats to our way of life.

There are more foreign spies and their proxies operating in Australia than there were at the height of the Cold War.

Foreign governments are seeking information about Australia's capabilities, research and technology, and domestic and foreign policy.

This year, for example, ASIO discovered and disrupted a plot to penetrate Australia's intelligence community.

An Australia-based foreign national was working with a team of foreign intelligence officers, who were trying to recruit multiple Australian security clearance holders. The agents wanted sensitive information about the intelligence community's operations, particularly those directed against their home country.

While the concept of espionage is well known, 'foreign interference' is often misunderstood. Simply praising a foreign country or publicly taking its side is not, of itself, foreign interference.

But when the advocacy is being covertly orchestrated by a foreign government and is contrary to Australia's national interest, it may well constitute foreign interference.

Almost every sector of Australian society is a potential target of foreign interference, and the threat manifests itself in different but equally unacceptable ways.

In 2019–20, ASIO stepped up its investigations into attempts to secretly co-opt current and future Australian

politicians. In all states and territories, at every level of government, intelligence services are seeking to cultivate politicians who will advance the interests of the foreign country.

Foreign interference also manifests in the monitoring, harassing and intimidating of Australia's culturally diverse communities.

We have uncovered many cases—involving multiple countries—where Australian community members and their families have been threatened for expressing views at odds with the foreign government's policies or values.

It is unacceptable that people in Australia are being intimidated simply for advocating democratic reforms or criticising human rights abuses. Seen in this context, foreign interference can be nothing less than an attack on Australia's sovereignty, multicultural communities, values and freedoms.

## Performance

This year has been a challenging time for all Australians. ASIO has continued to perform well under difficult circumstances, and my team has shown professionalism and dedication to our mission to deliver outstanding results.

Working with our law enforcement partners, ASIO's intelligence led to terrorist arrests, convictions and disruptions.

In addition to our actions directly targeting espionage and foreign interference, we continued to provide government and industry with trusted advice to help them protect themselves.

We know our efforts have been successful because we have seen foreign intelligence services reassessing the risks of operating in Australia, and in some cases ceasing their activities.

Close readers of this report may notice changes to our staffing and structures. This year, I took the opportunity to clarify the lines of authority and responsibility in our senior workforce.

The number of senior executive officers is now more appropriate for an organisation of ASIO's size. One consequence of these reforms was a further improvement in the proportion of women in senior roles. For example, women now make up 60 per cent of our Executive Committee.

## Transparency

As Director-General, I am committed to ensuring we don't just do what it is legal, we do what is right.

ASIO recognises we are granted extraordinary powers. We must use these responsibly, and be accountable to Australians and their parliament. This is why new Minister's Guidelines were issued this year, updating the legal obligations placed on ASIO to make sure our work is lawful, proportionate and ethical.

During the reporting period, we met with the Inspector-General of Intelligence and Security (IGIS) on at least a bi-monthly basis, supported by fortnightly meetings with senior staff from the Office of the IGIS. The IGIS possesses powers akin to a standing royal commission and is a key pillar of our rigorous oversight framework.

I intend to be as open as I can be about ASIO's work. This reflects my personal belief in the power of transparency, a desire to dispel myths about our Organisation, and the importance of explaining the true nature of the threats facing our country.

In 2019–20, ASIO provided nine unclassified submissions to the Parliamentary Joint Committee on Intelligence and Security, and appeared before five of its public hearings. ASIO also appeared before a Senate inquiry into press freedom and a public hearing on Australia's telecommunications access legislation conducted by the Independent National Security Legislation Monitor. In February, I delivered my first Annual Threat Assessment. We also began implementing a strategy to take our Organisation into the spotlight of social media.

This report will provide further context to the work ASIO's people do every day to protect Australia and Australians from threats to their security. We are your security service. And we make a difference.



**Mike Burgess**

Director-General of Security







# 2

## Overview of ASIO

---

# At a glance

## Commitment to legality and propriety

p. 9

ASIO must operate lawfully, in proportion to the threats we are investigating, and in line with the standards and expectations of the Australian community. We don't just do what it is legal, we do what is right.

# Overview of ASIO

ASIO protects Australia and Australians from threats to their security.

Our functions are set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act):

- a. to obtain, correlate and evaluate intelligence relevant to security;
- b. for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;
- c. to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities.
  - ca. to furnish security assessments to a State or an authority of a State in accordance with paragraph 40(1)(b);
- d. to advise Ministers, authorities of the Commonwealth and such other persons as the Minister, by notice in writing given to the Director-General, determines on matters relating to protective security; and
- e. to obtain within Australia foreign intelligence pursuant to section 27A or 27B of this Act or section 11A, 11B or 11C of the *Telecommunications (Interception and Access) Act 1979*, and to communicate any such intelligence in accordance with this Act or the *Telecommunications (Interception and Access) Act 1979*; and

- f. to co-operate with and assist bodies referred to in section 19A [of the ASIO Act] in accordance with that section.

In 2019–20, we pursued our purpose through four key activities:

- countering terrorism;
- countering espionage, foreign interference, sabotage and malicious insiders;
- countering serious threats to Australia's border integrity; and
- providing protective security advice to government and industry.

Part 4 of this report summarises our performance in relation to these key activities during 2019–20.

## Commitment to legality and propriety

ASIO must operate lawfully, in proportion to the threats we are investigating, and in line with the standards and expectations of the Australian community. We don't just do what it is legal, we do what is right. ASIO is subject to rigorous oversight, including by the Inspector-General of Intelligence and Security, who has powers akin to a royal commission.

ASIO’s accountable authority

Name	Position title/ position held	Period as the accountable authority within the reporting period	
		Date of commencement	Date of cessation
Mike Burgess	Director-General of Security	15 September 2019	N/A
Duncan Lewis AO DSC CSC	Director-General of Security	14 September 2014	14 September 2019

Mr Mike Burgess, Director-General of Security, is ASIO’s accountable authority. He has been Director-General of Security since 15 September 2019.

We need people who can out-think  
and out-imagine our adversaries  
to achieve our mission of protecting  
Australia and Australians. We also  
need to ensure that our workforce  
continues to mirror the diversity  
of the society we serve.

# Out-thinking Australia's adversaries

In a complex, challenging and changing security environment, our success is built on the imagination and intelligence of our team. ASIO's people are ordinary Australians but they do extraordinary things—they are our most important asset. All our teams contribute to our mission.

## Who are the people of ASIO?

ASIO staff are carers, parents, grandparents and community volunteers and come from various backgrounds, including music; teaching; geology; nursing; and science, technology, engineering and maths (STEM). We are proud Aboriginal and Torres Strait Islander peoples and second- or third-generation Australians. We are introverted, extroverted and neurodiverse. We are tradespeople, as well as technical, corporate and intelligence professionals. We are your neighbours and part of your community. The only difference is that we don't tell you where we work, what we do, or how we do it.

## Our skills

Our people need to out-think and out-imagine our adversaries. Being an ASIO officer requires the ability to be open-minded and the confidence to work both independently and as part of a team. Our people are engaging, are deeply analytical, and have foreign language, legal, and international and domestic politics skills. Some work in engineering and information technology, others in finance and human resources.

## A diverse workplace

We seek to reflect the diversity of the community we protect. We want every ASIO officer to bring their unique skills, experience, perspectives and whole selves to work. In 2019–20 we recruited 141 staff. Our career opportunities are open to all.

# Organisational structure



Figure 1: ASIO’s organisational structure at 30 June 2020

Strategic Advisor



**Hazel Bennett**  
Enterprise Service Delivery

Legal Services	Technology & Reform	Enterprise Services	Strategy & Engagement
Assessments, Corporate Law & Capability Protection	Infrastructure	Finance & Procurement	Governance & Strategy
Operations Law & Litigation	Business Information Services	Internal Security Services	Government Engagement & Oversight
	Data	People	
	Reform	Learning & Development	
		Facilities Services	
		Investment	

- Band 3
- Band 2
- Band 1







# 3

**Australia's  
security  
environment  
and outlook**

---

# At a glance

## Terrorism

p. 17

Australia's national terrorism threat level remains at **PROBABLE**. The primary threat remains Sunni Islamic extremism, but other violent ideologies—such as those of the extreme right—are also of concern.

p. 23

The threat to Australia from foreign states seeking to obtain strategic advantage at the expense of Australia and its interests cannot be understated.

# Australia's security environment and outlook

## Terrorism in Australia

Australia's national terrorism threat level remains at **PROBABLE**—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct a terrorist attack in Australia.

Although COVID-19 has changed our environment, it has not substantially diminished the threat of terrorism in Australia. The primary threat remains Sunni Islamic extremism, but other violent ideologies—such as those of the extreme right—are also of concern.

Islamic extremists continue to disseminate propaganda designed to radicalise, recruit, instruct on and inspire terrorist attacks, including in Australia. Australia continues to be specifically mentioned in pro-Islamic State of Iraq and the Levant (ISIL) propaganda, and these releases add to a large body of material that encourages terrorism. This propaganda is drawing a younger audience which accesses this material online, and its potential reach increased in 2020 as COVID-19 social isolation increasingly pushed Australians online. Al-Qa'ida remains active, particularly offshore; although in the next five years Australian prisons are due to release a number of Islamic extremist prisoners whose actions were inspired by al-Qa'ida.

Extreme right-wing groups and individuals have been in ASIO's sights for many decades—while we have maintained continuous and dedicated resources to this area, extremists such as neo-Nazis represent a serious, increasing and evolving threat to security. The 2019 Christchurch attack continues to be drawn on for inspiration by right-wing extremists worldwide.

These groups are also becoming ideological: more aware of and committed to specific dogmas, philosophies and views. They draw from a diversity of ideas and are attracting a younger membership who display few overt signs of their extremist ideology.

## Right-wing extremism

While ASIO has a longstanding and enduring interest in investigating and advising on the threat from both right-wing and left-wing extremists, this year saw an increased growth in ASIO investigations related to extreme right-wing groups, individuals and emerging ideologies. Australia is not unique in this regard; other Western countries have also increased their focus on this issue while maintaining counter-terrorism programs against transnational terrorist groups such as al-Qa'ida and ISIL. In the last year:

- extreme right-wing individuals comprised around a third of all ASIO counter-terrorism investigative subjects;
- investigations relating to these individuals occurred in all Australian states and territories;
- a right-wing extremist charged under Commonwealth terrorism laws in 2016 was found guilty of terrorism offences including 'acts in preparation for, or planning a terrorist act';
- for the first time, a right-wing extremist was prevented from travelling offshore to fight on a foreign battlefield, due to a passport cancellation based on an ASIO adverse security assessment;
- the second terrorism disruption, in Australia, linked to an individual with an extreme right-wing ideology occurred; and
- our subject matter experts provided over 50 briefings and presentations on this issue at the request of partners and clients.

The COVID-19 pandemic has been used by right-wing and issue-motivated extremists to promote their views. They are seeking to exploit social and economic dislocation; and their extremist ideology has been

spreading more quickly and widely as Australians spend more time online engaging with like-minded individuals. However, calls for violence and sabotage have not yet been acted on in Australia.

Violent extremists remain attracted to 'soft' targets, such as crowds in public places. While the symbolic appeal of attacking a government or authority—such as the military, police and security agencies—remains, easily accessible targets reduce the capability required for an attack.

Any terrorist attack in Australia for at least the next 12 months is more likely to be committed by a single person or a small group using simple methods. The use of basic weapons, improvised explosives and firearms remains more likely. But terrorists are creative—they could use new and innovative weapons and tactics, and more sophisticated attacks are possible.

### **Terrorism—the international security environment**

The legacy of ISIL's caliphate—foreign fighters and their families, its global network, and the availability of propaganda inciting violence—still shapes the global environment.

Through its affiliates, al-Qa'ida continues to embed itself in local conflicts and exploit weak governance, and has not relinquished its longstanding anti-Western ambitions.

Further, the emergence of nationalist and isolationist narratives globally is normalising aspects of extreme right-wing ideology.

### **Europe and North America**

Europe and North America remain terrorist targets, posing a threat of incidental harm to Australians there. During 2019–20, Islamic and right-wing extremist attacks occurred in Europe and North America; many other attacks were thwarted.

Attacks are most likely to be inspired by Islamic extremist ideology and use basic weapons such as knives and vehicles, firearms or explosives to target crowded places or police and uniformed personnel. The release of terrorist prisoners across Western Europe is likely to exacerbate the terrorist threat.

Right-wing extremists primarily pose a threat to Jewish, Muslim or other minorities, as well as extremists' ideological opponents. Extremist rhetoric and previous attacks can inspire action from individuals with little or no connection to established extreme right-wing groups.

COVID-19 has energised some issue-motivated extremists in North America, but has not measurably changed the terrorist threat there or in Europe. The pandemic's longer term effects are yet to be seen.

## South-East Asia

The terrorist threat in South-East Asia remains elevated. South-East Asian ISIL affiliates continue to be influenced by ISIL's ideology, narrative and global jihadist attack methodology. Despite the death of former ISIL leader Abu Bakr al-Baghdadi, and a number of significant disruptions, pro-ISIL groups and individuals in Indonesia, Malaysia and the Philippines have continued their campaigns of plots and attacks in support of ISIL and local extremist agendas. Although ISIL continues to dominate the regional threat environment, al-Qa'ida-aligned groups also continue to exist in South-East Asia, recruiting and training to prepare for possible future acts of violence.

Cross-border connections, both within the region and into international conflict zones, increase the risk of the transfer of skills, attack methodologies and ideological influence from transnational Islamic extremist groups. Despite COVID-19 restrictions largely constraining extremists' movements, those in South-East Asia are increasingly collaborating and consuming ISIL propaganda online, as well as planning and conducting simple, often opportunistic, attacks primarily directed against local security forces and sectarian targets. Under ISIL's influence, Islamic extremists are adapting their methods, with suicide bombings becoming more common in the southern Philippines.

Many South-East Asians who travelled in large numbers to join ISIL and al-Qa'ida-aligned groups in Syria and Iraq returned early in the conflict with greater capability, ideological commitment and status.

The scheduled release of terrorist detainees in South-East Asia, many of whom probably maintain an extremist ideology, will also be detrimental to the security environment in the region.

## South and Central Asia

Islamic extremists retain the freedom to operate in less-governed areas of Afghanistan and Pakistan. Their frequent attacks on government interests, security forces and minorities will continue. Islamic State—Khorasan Province in Afghanistan has transitioned to a clandestine insurgency after losing territory, but its high-profile attacks persist. Elsewhere in the region, Islamic extremist ideology is still radicalising individuals and groups who conduct low-capability attacks.

The full impact of COVID-19 has not yet been realised; however, it has had limited effect on the terrorist threat in South Asia to date. While decreased tourism reduces the likelihood of Westerners being attacked, the anti-Western intent of some extremists is unchanged.

## Middle East

ISIL's post-caliphate insurgency continues in Syria and Iraq. Although ISIL has not reclaimed territory, and is still losing senior leaders and fighters, the ISIL threat in both countries persists. ISIL is still active elsewhere in the Middle East, although its strength varies. Online propaganda is a key tool and still resonates with disenfranchised individuals who can quickly mobilise to violence, including attacking Westerners.

Al-Qa'ida-affiliated or linked groups are still exploiting civil strife and ungoverned spaces. Their presence in Yemen and north-west Syria is an enduring threat to Western interests. Elsewhere, individuals and groups, driven by various ideological objectives—some backed by Iran—have attacked targets in Egypt, Turkey, Israel and the Palestinian Territories, Saudi Arabia and Yemen.

While COVID-19 has not significantly changed terrorist threats in the Middle East so far, its longer term effects are not yet clear. Travel restrictions have temporarily reduced the exposure of Australians, but terrorists' intent to attack Australia is unlikely to change.

### Africa

In Africa, established al-Qa'ida-aligned and ISIL-aligned groups continued their campaigns of attacks aimed at destabilising regional governments. Most target Westerners, including Australians, if they have the opportunity. Emerging ISIL affiliates have survived counter-terrorism operations and in some cases gained strength, including in northern Mozambique where one affiliate group operates close to Australian mining operations.

Mali-based terrorist groups have increased their areas of operation, including into Burkina Faso where 19 local employees of an Australian-owned company were killed in November 2019 when a mining convoy was ambushed.

### Border integrity

Australia continues to see suppressed demand for irregular maritime ventures to Australia, due to the continued view held by potential irregular immigrants (PII) that there is a low prospect of permanent resettlement in Australia. Despite this, attempts at irregular maritime migration to Australia and within the region occurred throughout the period, albeit at low levels.

Deteriorating economic, health or security conditions in traditional PII source countries have the potential to drive individuals to take desperate measures to escape such conditions in the future, possibly through irregular migration to Australia. This remains a concern; however, to date, COVID-19 has further suppressed demand for irregular migration as closed borders, strict lockdown measures and restricted international and domestic travel in PII source countries create a difficult operating environment for people smugglers. Similarly, reduced incomes and employment opportunities for PII in the current environment limit their ability to access irregular migration pathways, as their focus is on more immediate needs.

## Communal violence and violent protest

Communal violence in Australia is infrequent. Communal tensions are generally expressed through public events and demonstrations aimed at drawing the attention of the broader Australian community to specific issues.

There is a limited tradition of violent protest in Australia. While incidental violence has occurred in the past 12 months, most protest continues to resolve peacefully. Violence is most likely when events are attended by counter-protesters.

## Premeditated violent protests

ASIO can investigate protest activities only where premeditated violence may be used, or where tactics used are likely to result in violence.

Although large-scale protests have taken place throughout the past 12 months, violent protest in Australia remains rare. The use of provocative and disruptive tactics, which occurred during some environmental protests in 2019, are more likely. Tactics such as obstructing pedestrians and traffic are designed to create economic disruption and draw the broader community's attention to a cause.

At times, protests have resulted in incidental violence or property damage. Such incidental violence, rather than premeditated violence, remains a matter for police.



## Espionage and foreign interference

Australia remains a target for acts of espionage and interference by foreign states, who continue to target government, academia and industry for access to sensitive and valuable information.

These acts, which occur on a daily basis, are of unprecedented scale and sophistication. The threat to Australia from foreign states seeking to obtain strategic advantage at the expense of Australia and its interests cannot be understated. The intent is to engineer fundamental shifts in Australia's position in the world, not just to collect intelligence or use Australia as a potential 'back door' into its allies and partners. There are more foreign intelligence officers and their proxies operating in Australia now than at the height of the Cold War, and many of them have the requisite level of capability, intent and persistence to cause significant harm to Australia's national security.

This threat encompasses a widening range of activities, combined with clear intent by foreign states to shape Australia's policies, decisions and actions to their benefit. We continue to observe—and actively seek to mitigate—clandestine interference and penetration efforts by intelligence services from a range of nations against all levels of Australian government.

The consequences of unchecked espionage and foreign interference are grave: they damage Australia's economy and international competitiveness, harm its alliances, undermine its governments and erode its capacity to make decisions in its own national interest. They also threaten the safety of Australians.

Foreign governments continue to attempt to interfere in Australia's culturally and linguistically diverse communities. Some foreign governments seek to control or suppress opposition or dissent which they perceive as a threat. Such interference has included threats of harm to individuals and/or their families, both in Australia and abroad.

Alternatively, foreign governments use community members to monitor, direct and influence the activities of these communities in Australia.

Foreign government espionage and interference activities against Australians do not occur only on Australian soil. Cyber espionage is targeting all levels of government, universities and academia—and Defence-related and corporate information networks—to gain access to sensitive and commercially valuable information. As a relatively low-risk, scalable and at times non-attributable means of obtaining privileged and timely information, it is an attractive tool by which foreign intelligence services (FIS) can target Australians.

## Espionage

Espionage is the theft of Australian information or capabilities with the intent of providing that information or capability to another country.

Such activity may threaten Australia's national security or provide a political, commercial or economic advantage to another country.

Espionage activities can be directed against Australian governments, Defence, politics, industry, foreign relations or commerce; or other information or objects that are otherwise unavailable to a foreign nation.

The growth in the number of Australians working from home during the global COVID-19 pandemic has increased Australia's exposure to a range of hostile actors in cyberspace. As businesses move to remote access options for employees working from home, motivated state and non-state malicious cyber actors may attempt to take advantage. ASIO advice, shared with academic and corporate sectors through our Outreach program, plays an important role in helping to mitigate the cyber security risks associated with Australia's increased online presence and remote working arrangements.

FIS are seeking to recruit Australians online through social media platforms—taking advantage of the low cost and ease of disguising their approach to their targets. Many of the attributes that make social media so valuable also make it vulnerable; as a result, FIS are seeking to take advantage of these targeting opportunities.

Australians overseas are also targeted by FIS for their current or future potential to undertake espionage and foreign interference activities on behalf of FIS. In some instances, FIS approach Australians through professional networking sites, seeking non-public or sensitive information under the guise of representing think tanks and recruitment agencies. FIS also entice Australians to travel overseas where they are more vulnerable—FIS use their home ground advantage to cultivate and recruit Australians for espionage or foreign interference activities.

## Foreign interference

Foreign interference is detrimental to Australia's values, interests and security.

Unlike legitimate 'soft power' lobbying or diplomatic activity, foreign interference involves covert, deceptive or threatening actions on behalf of, in collaboration with, or directed by a foreign principal.

ASIO has identified foreign state actors and their proxies persistently seeking to develop relationships with Australian Government political figures, academia, commercial interests and individuals, in pursuit of objectives detrimental to Australian interests.

These activities are unacceptable.

ASIO works across government to harden Australia's critical infrastructure against harm from FIS—particularly FIS efforts that target critical infrastructure, sensitive and sizeable Australian data sets, and emerging technology.

Australia's telecommunications sector is an attractive target, and its security is of utmost importance. It underpins Australia's critical infrastructure and way of life. Access or disruption to the sector provides opportunities for Australia's adversaries to conduct activities which threaten Australia's national security.

ASIO plays an important role in helping to mitigate the risk that foreign investment may pose to Australia's security, including by providing advice to the Foreign Investment Review Board (FIRB). Foreign investment continues to play a vital role in Australia's economic success, stability and prosperity, and fully assessing any associated national security concerns benefits both the investor and Australia.

In addressing these challenges, we seek to 'detect and protect' by hardening the security environment against hostile foreign actors. We and our national security partners actively conduct counter-foreign interference operations—increasing our adversaries' costs and risk, thereby reducing the harm they cause. We also deploy an array of measures to identify and respond to espionage operations directed against Australia.



# 4

**Report on  
performance**



---

# At a glance

## Analysis of our performance

**p. 53**

We achieved our purpose during the reporting period through the delivery of three key services: identifying and mitigating efforts to harm Australians and Australia; providing intelligence and advice to enable better decision-making; and building our partners' security and intelligence capabilities.

# Annual performance statement 2019–20

## Introductory statement

I, as Director-General of Security and the accountable authority of ASIO, present the 2019–20 annual performance statements for ASIO, as required under subsection 39(1)(a) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). In my opinion, these statements accurately present the performance of ASIO in achieving its purpose and comply with subsection 39(2) of the PGPA Act.

A handwritten signature in black ink, appearing to read 'Mike Burgess', with a stylized, cursive script.

**Mike Burgess**

Director-General of Security

## ASIO's purpose

ASIO protects Australia and Australians from threats to their security. Our purpose, as defined in ASIO's Corporate Plan 2019–20, is to protect Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty. In 2019–20, ASIO achieved this purpose by focusing on three strategic objectives—Counter, Shape and Build—in four 'key mission' areas:

- counter-terrorism;
- counter-espionage and foreign interference;
- border integrity, including people smuggling; and
- protective security advice.



## Results for 2019–20

The results in this report address the performance criteria contained in ASIO's Portfolio Budget Statement (PBS): 'advice that assists the Australian Government, government agencies and industry to manage security risks and disrupt activities that threaten Australia's security'.

The measures used to assess our performance against the strategic objectives are outlined in ASIO's Corporate Plan 2019–20.

As in recent years, in 2019–20 we commenced a comprehensive survey of external stakeholders to complement other performance assessment and reporting inputs. In March 2020, with the onset of the COVID-19 global pandemic, ASIO decided not to proceed with the survey for 2019–20 because of health and safety considerations. Instead, we adapted our assessment and reporting methods to those most practicable and appropriate for this annual performance report.

# Key mission 1: counter-terrorism

## PERFORMANCE OBJECTIVE

## Counter

We identify and mitigate violent, clandestine or deceptive efforts to harm Australians and compromise Australian sovereignty, economic wellbeing and national security.

## 2019–20 RESULT

## Achieved

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

### Identifying and disrupting terrorism-related threats to Australians and Australian interests

In 2019–20, ASIO intelligence made a direct contribution to identifying and disrupting terrorism-related threats to Australians and Australian interests. Notable disruptions informed by ASIO investigations included the following.

- On 4 December 2019, an individual was arrested in Sydney and subsequently charged with ‘other acts done in preparation for, or planning, terrorist acts’ and other terrorism offences.
- On 14 March 2020, an individual was arrested, on the New South Wales south coast, who was subsequently charged with ‘other acts done in preparation for, or planning, terrorist acts’.

ASIO’s support to the Joint Counter-Terrorism Teams (JCTT)<sup>1</sup> assisted with the prosecution and sentencing of the following individuals for terrorism and related offences.

- On 21 May 2020, Melbourne-based Ali Khalif Shire Ali was sentenced to 10 years imprisonment after pleading guilty to a charge of an act in preparation for, or planning, a terrorist act. Ali had enquired about gaining access to a firearm and ammunition in preparation for an attack planned to take place in Federation Square, Melbourne, in late 2017.

<sup>1</sup> Joint Counter-Terrorism Teams (JCTT) are multi-agency bodies made up of the Australian Federal Police (AFP), ASIO and state-based police agencies, supported by other Commonwealth and state-based agencies such as Australian Border Force, Australian Criminal Intelligence Commission (ACIC) and state Justice Departments. JCTTs operate in all Australian jurisdictions. They were established to conduct counter-terrorism operations, with the intention of disrupting terrorism and/or bringing criminal prosecutions for breaches of terrorism legislation. Each JCTT is a critical tool for managing the investigation, disruption and prosecution of terrorist activity in Australia.

- On 7 April 2020, an individual was found guilty at retrial of acts in preparation for a terrorist act. This concluded a JCTT investigation that commenced in Sydney in 2016 with the arrest of two 16-year-olds who were detected carrying knives in a public place and later charged with terrorism offences.
- On 5 December 2019, Melbourne-based Philip Galea was found guilty of ‘acts in preparation for, or planning, a terrorist act’, and attempting to make a document likely to facilitate a terrorist act. These offences related to a plot to attack various sites linked to left-wing causes in Melbourne. This marked the first time that an individual with an extreme right-wing ideology had been convicted under Australia’s counter-terrorism laws.
- On 29 November 2019, three individuals, who had been convicted of engaging in a terrorist act after conducting an arson attack on a Shia mosque, received lengthy sentences. In consideration of additional terrorism offences for a separate plot to conduct an attack on or around Christmas Day 2016 in Melbourne’s central business district, Ahmed Mohamed and Abdullah Chaarani were each sentenced to 38 years in prison and Hamza Abbas was sentenced to 22 years. A fourth individual, Ibrahim Abbas, who pled guilty for his involvement in the Christmas Day plot, was sentenced to 24 years imprisonment.

### Advice informs national mitigation measures

Throughout the reporting period, our intelligence and advice informed national measures and whole-of-government efforts to mitigate the terrorist threat to Australians and Australian interests. Notable examples include providing:

- security advice which informed decisions to impose Temporary Exclusion Orders on a small number of Australians of counter-terrorism interest located overseas, enabling a more controlled return of these individuals to Australia;
- assessments which informed decisions to cancel Australian passports of individuals linked to extremist groups in the Syria/Iraq conflict and right-wing extremist groups offshore. The passports were cancelled either to prevent travel to conflict regions or to limit the ability of individuals already offshore to travel to a third country;
- intelligence reporting informing the listing of IS-Somalia and the relisting of al-Qa’ida in the Arabian Peninsula, al-Qa’ida in the Indian Subcontinent, IS-Libya, and IS-Sinai Province as terrorist organisations under Part 5.3 of the Criminal Code;
- assessments on global terrorist threats that informed Department of Foreign Affairs and Trade (DFAT) public travel advisories and measures to protect Australian interests overseas;
- threat assessments that informed threat mitigation strategies for crowded public places, and measures to protect Australian critical infrastructure—including aviation, maritime and government facilities;

- threat assessments, including on terrorist weapons and tactics and the ongoing threat posed by ISIL and al-Qa'ida, to inform federal, state and territory security responses; and
- assessments to AusCheck to enable it to mitigate the threat associated with individuals of security concern gaining access to security-controlled places.

During the reporting period, we provided:

- 136 268 access security assessments to AusCheck, including for individuals seeking Aviation Security Identification Cards (ASICs) and Maritime Security Identification Cards (MSICs);
- 7344 assessments for T20 Cricket World Cup Special Event accreditation; and
- 12 192 access security assessments of individuals seeking access to security-sensitive chemicals or nuclear sites.

## Mitigating the extremist threat

A former Australia-based individual travelled overseas in December 2014. ASIO subsequently received reporting indicating that by early 2015 the individual had entered Syria and joined ISIL, received militant training, and engaged in fighting on behalf of the group. It is likely he remains in Syria.

Our investigations revealed that this individual may also be involved in financial facilitation on behalf of ISIL. We further determined that he remained in contact with his Australia-based family and associates and, through them, might have sought to raise further funds to finance ISIL activity.

In July 2019, the JCTT Canberra conducted overt enter-and-search operations under ASIO warrant relating to this individual's Australia-based family and associates and their financial support for ISIL. Separately, ASIO shared intelligence on the individual's activities and intentions with other Commonwealth agencies, who drew on this advice to develop mitigation activities. As a result of our—and others'—mitigation activities, this individual's ability to raise further funds for ISIL is now limited, and their appeal to others in the community who are seeking to provide support to extremist groups overseas has been reduced.

**PERFORMANCE  
OBJECTIVE**

## Shape

**2019–20 RESULT**

## Achieved

**We provide Australian governments, law enforcement and industry with intelligence and advice to enable better decision-making in relation to security responses, policies and priorities, including warning of emerging and imminent threats.**

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

We achieved our objective to enable better decision-making through the provision of intelligence and advice during the reporting period, with our assessments on the terrorism threat environment continuing to be in high demand from our Commonwealth, state and territory policy, security and law enforcement partners. During the reporting period, we published 898 intelligence and security reports on a wide range of local and international terrorism-related matters, with the following being of particular note.

- We provided support to the High Risk Terrorist Offenders (HRTTO) scheme, established in response to the substantial number of terrorism offenders scheduled for release from Australian prisons over the next five years. Our advice contributed to whole-of-government considerations under the HRTTO scheme to ensure the threat posed by recent (and upcoming) releases of convicted terrorist offenders is appropriately understood and managed.
- Our assessments on the increasing prevalence of extreme right-wing groups in Australia and overseas—including on the promulgation of online propaganda, associated indicators and international context—enabled law enforcement stakeholders to develop mitigation strategies.
- We provided advice on the impact of the COVID-19 pandemic on the Australian security environment. This product received positive feedback from stakeholders, and was used by the Office of National Intelligence (ONI) to inform its evaluation processes.
- We adapted product distribution processes to ensure customers could continue to access advice, including key partner agencies which had adopted work-from-home arrangements as a consequence of COVID-19.

In our role as Counter-Terrorism Intelligence Mission lead, in late 2019 we launched an updated counter-terrorism prioritisation and evaluation framework, providing clear direction on Australian counter-terrorism priorities to the National Intelligence Community (NIC). The framework aims to ensure all counter-terrorism capabilities are directed at the highest intelligence priorities. It also provides a means by which to measure and evaluate counter-terrorism effort, ensure maximum agility and responsiveness in a rapidly changing security environment, and guide resource allocation and capability development across the NIC. The intelligence priorities, which are formally reviewed and evaluated quarterly, are developed with multi-agency input. Stakeholders, including Australian intelligence and law enforcement partners, provided positive feedback on the launch of the updated framework.

**PERFORMANCE  
OBJECTIVE**

**We work with our Australian and international partners  
to build security and intelligence capabilities.**

## Build

**2019–20 RESULT**

## Achieved

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

Throughout 2019–20, our counter-terrorism activities informed international and domestic partner capability, including government, security and industry partners. Our achievement of this objective is demonstrated by the following.

- ASIO contributed to the ongoing review of national guidelines and strategies within the Australia-New Zealand Counter-Terrorism Committee (ANZCTC) framework, including the 2019 review of the *National counter-terrorism handbook* and the 2020 review of the National Counter-Terrorism Strategy. We also continued to inform and build the ANZCTC's decision-making and capability development through the following activities.
  - We provided subject matter experts to present at security and counter-terrorism training courses, including ANZCTC Skills Enhancement Courses and training courses conducted by law enforcement and partner agencies.
  - We developed scenarios, exercise products and other supporting materials to help law enforcement and defence partners to plan and conduct counter-terrorism exercises. We also actively participated in exercises with partners to enhance interoperability and information flows.
- Like many other agencies, ASIO experienced challenges in the operating environment posed by COVID-19 and the subsequent physical distancing requirements. In response to restrictions in the operating environment, our operational teams developed and applied innovative techniques to ensure their activities could continue, while maintaining the security of our operations and ensuring the health and safety of our officers and human sources. We shared details of these techniques with Australian partners, and jointly developed additional capability to be shared with one of our law enforcement partners.

- We provided vulnerability assessment security reviews and security zone briefings to government agencies and critical national infrastructure clients, including defence industry. Our advice also contributed to Australian Signals Directorate (ASD) certification of Gateway Service Provider facilities in Australia, which certifies the physical security of ICT equipment, systems and facilities.



## Key mission 2: counter-espionage and foreign interference

### PERFORMANCE OBJECTIVE

## Counter

We identify and mitigate violent, clandestine or deceptive efforts to harm Australians and compromise Australian sovereignty, economic wellbeing and national security.

### 2019–20 RESULT

## Achieved

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

ASIO successfully identified new high-harm espionage and foreign interference (EFI) activities, and directly supported disruption activities and other mitigations. We leveraged our expertise on foreign intelligence activities in Australia, and used our extensive suite of investigative tools, to work with partners in countering EFI threats against Australian interests.

Our efforts towards achieving this measure included:

- conducting discovery work leading to the identification of previously undeclared FIS personnel and activities in Australia. This has enhanced our understanding of the current EFI threat, allowing for more targeted investigative and operational activity and informing mitigation and disruption planning;
- identifying cyber espionage activities directed against Australian interests, enabling responses and countermeasures to be put in place by the appropriate Australian Government authorities;

- working closely with key partners, taking proactive and direct action to disrupt harmful EFI threats to Australian interests, against the backdrop of the global uncertainty caused by the COVID-19 pandemic. This included responding to threats to the integrity of Australia's political democratic systems, institutions and processes; Australia's tertiary sector; and social cohesion across Australian communities; and
- providing targeted, actionable advice which enhanced the Australian Government's defensive posture and preparedness, helping to protect against emerging EFI threats.

The ASIO-led, multi-agency Counter Foreign Interference Taskforce (CFITF) has built its capacity to identify and respond to possible acts of foreign interference and espionage. Established in early 2020, the CFITF works to disrupt and deter hostile actors attempting to undermine Australia's national interests through foreign interference and espionage.

### Personnel security assessments

Our personnel security assessments continued to play a pivotal role in assisting the Australian Government to identify and mitigate violent, clandestine or deceptive efforts to compromise Australia's national security.

In 2019–20, we completed 34 035 personnel security assessments, comprising 30 383 assessments for Baseline, Negative Vetting (NV) 1 and 2 clearances and 3652 Positive Vetting (PV) clearances. This is an increase of over 1140 completed assessments compared with the previous year. Feedback from key stakeholders acknowledged our responsiveness, our level of engagement, and the relevance of advice provided.

The Australian Government Security Vetting Agency (AGSVA) continued to provide favourable feedback, and stated that—with ASIO's assistance—its progress towards the key performance benchmark set by government was a significant achievement.

We also completed a number of adverse and qualified personnel security assessments, containing information and recommendations about an individual's suitability to be granted or continue to hold a clearance. Key stakeholder feedback noted that, as a result of these assessments, agencies were able to issue security clearances to staff in a timely manner and, where needed, mitigate security risks.

## Countering espionage

Our investigative and operational efforts continue to mitigate the espionage threat from hostile foreign intelligence services (FIS) targeting Australia. Most notable was our disruption of an Australia-based foreign national who was assisting a team of foreign intelligence officers.

These officers were operating to penetrate the Australian Government and the National Intelligence Community (NIC) by seeking to recruit a number of Australian security clearance holders who could provide them with access to classified Australian Government information.

Their primary goal to covertly acquire classified information about the NIC's current operations and capabilities, especially those directed against their nation state, would potentially have granted their government significant strategic advantage over Australia. We conducted overt activity against the Australia-based foreign national and the officer network, which thwarted the foreign intelligence operation and prevented the passage of classified information to the FIS.

**PERFORMANCE  
OBJECTIVE**

## Shape

**2019–20 RESULT**

## Achieved

**We provide Australian governments, law enforcement and industry with intelligence and advice to enable better decision-making in relation to security responses, policies and priorities, including warning of emerging and imminent threats.**

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

Our intelligence advice continued to be instrumental in enhancing the Australian Government's security awareness of EFI threats. This has informed security-related policy and risk mitigation, resulting in a more resilient Australia. We produced 51 assessments, containing intelligence analysis on known threats and threat actions, including in areas of specific government focus.

- We provided advice to Australian Government stakeholders, which informed the development and consideration of new legislative and regulatory measures designed to increase transparency and combat foreign interference in Australia's democratic institutions and processes, and across key economic sectors.
- We informed the Foreign Investment Review Board's (FIRB) considerations by providing assessments on the threats posed to Australia's national security from a number of proposed foreign investments.
- We translated insights derived from our investigations into practical security advice and worked closely with key partners—in particular, the Office of the National Counter Foreign

Interference Coordinator within the Department of Home Affairs—to build resilience against EFI across key economic sectors.

- We identified opportunities to improve processes for identifying and assessing risks to infrastructure sectors, and worked with the Department of Treasury and other agencies to develop more effective whole-of-government arrangements.
- We also collaborated with the Australian Cyber Security Centre within ASD, on the identification of—and responses to—emerging cyber threats, drawing on our knowledge of the threats posed by those seeking to undertake EFI activities against Australia through cyber or technical capabilities.

Further, we provided highly valued advice to government on the implications of the COVID-19 pandemic for the EFI and malicious insider threat landscape. This included practical steps that agencies could take to mitigate risks associated with modified working arrangements. This advice received positive feedback, particularly from the departments of Home Affairs and Defence.

### Personnel security assessments

We contributed significant security advice which shaped ongoing whole-of-government personnel security policy reforms throughout 2019–20. The reform program this year focused on issues concerning the eligibility, and ongoing suitability, of clearance holders. Our advice enabled government to make intelligence-led decisions on these matters to mitigate insider threat risks.



## The impact of legislative reform

The passage of espionage and foreign interference (EFI) legislation has proven a valuable tool to ASIO and partners in preventing threats posed by foreign intelligence services (FIS) and their proxies. The legislation, coupled with operational work, caused some intelligence services to reassess the risks associated with conducting clandestine foreign intelligence operations in or against Australia, and—in some cases—they ceased activities.

We assess that the legislation also contributed to some FIS more openly declaring their intelligence presence and activities in Australia. This informed our assessments, and improved our understanding of the EFI threat in Australia, enabling us to direct our efforts towards mitigating highest harm activities.

**PERFORMANCE  
OBJECTIVE**

**We work with our Australian and international partners  
to build security and intelligence capabilities.**

## Build

**2019–20 RESULT**

## Achieved

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

During the reporting period, we intensified efforts with domestic and international partners to build security and intelligence capabilities and support the development of counter-foreign interference capability across government.

- We delivered capability development programs for law enforcement partners and other affiliated agencies, to enhance our joint capacity to identify and actively disrupt harm from foreign interference.
- We enhanced our ability to identify and counter foreign interference through significantly improved cooperation and collaboration with NIC and foreign partners. This collaboration included the placement of several NIC agency staff in the newly established CFITF.
- We provided highly regarded protective security and defensive counter-espionage and interference advice to NIC and defence partners. Recipients informed us our advice helped shape organisational defensive counter-interference posture and programs, and enhanced collaboration with ASIO on security and insider threat matters.

- We extended capability-building activities across our technical, analytical and HUMINT platforms to key NIC partners including ASD, Australian Secret Intelligence Service (ASIS) and AFP.

ASIO also helped build resilience against FIS targeting.

- We provided protective security advice to government, and several industry and innovation sectors. This included personalised security advice for officials and representatives travelling overseas.
- We produced intelligence assessments and advice supporting the development of the University Foreign Interference Taskforce guidelines, and provided support to universities to implement the guidelines.
- We enhanced our information technology platform to increase the value of contact reports and case studies to our outreach and investigative programs.

Throughout 2019–20, we deepened relationships within the defence industry, and provided tailored advice and support to help partners secure their staff, information and facilities. In particular, this included working with them to identify supply chain risks and determine mitigation strategies. We are also developing additional information technology solutions to improve connectivity between Defence and ASIO, to amplify understanding of security threats and lead to better security outcomes.

### Personnel security assessments

We improved Australian Government efforts on vetting and personnel security matters by enhancing our engagement with partner agencies and providing clear, practical security advice. This included:

- helping government stakeholders to translate into practice lessons learned from international partners on global best practice for clearance maintenance and technology-derived efficiencies; and
- working closely with AGSVA and DFAT on projects to improve assessment times through electronic data transfer.

We also briefed AGSVA staff across Australia, which deepened their awareness of EFI threats and helped mitigate the trusted insider threat. After these briefings, which received positive feedback, we saw an increase in subscribers to our Outreach portal from Defence security staff and external vetting providers. Further, significant interest was expressed in our published product

on personnel security matters, with key stakeholders advising it had been used to develop several agency security measures including communication campaigns.

To build on this, we collaborated with partners on a strategy to guide the focus of future engagement, which will ensure that we continue to build our partners' security and intelligence capabilities and continue to provide useful, actionable assessments and advice.

## Key mission 3: border integrity, including people smuggling

### PERFORMANCE OBJECTIVE

### Counter

### 2019–20 RESULT

### Achieved

We identify and mitigate violent, clandestine or deceptive efforts to harm Australians and compromise Australian sovereignty, economic wellbeing and national security.

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

We achieved this objective by improving our prioritisation and assessment of lead information and referrals, by providing robust visa security assessments and security access assessments, and by giving actionable advice to external partners, including Home Affairs, DFAT and the AFP, as follows.

- We identified and mitigated national security risks by referencing our data holdings and producing security assessment of visa applicants referred to us by Home Affairs and DFAT. We also collaborated with stakeholders to enhance Australia's visa-screening processes and, in turn, to identify security issues and provide security advice to inform responses.
- We issued a number of adverse and qualified assessments, informing stakeholders' decision-making on the issuing or cancelling of visas, or the refusal of citizenship, to mitigate a range of national security risks.
- We assisted whole-of-government responses to threats to Australia's border integrity, providing a number of security assessments on whether Australian visa holders posed a security risk, including in relation to activities associated with people smuggling.

Table 1: Completed visa assessments

Type of entry	2017–18	2018–19	2019–20 <sup>2</sup>
Temporary visas	1746	1219	589
Permanent residence and citizenship	294	155	49
Onshore protection (air)	66	32	8
Offshore refugee/humanitarian	919	747	115
Illegal maritime arrivals	95	40	14
Other referred caseloads	2334	2121	1740
Resolution of national security border alerts	7353	7385	8530
<b>Total</b>	<b>12 807</b>	<b>11 699</b>	<b>11 045</b>

<sup>2</sup> In 2019–20 ASIO received fewer referrals for temporary visa assessments compared with previous years, resulting in fewer completed assessments.

We met service-level agreements with key stakeholders in producing these assessments. We worked closely with partners to find efficiencies which, combined with the impacts of COVID-19, resulted in a decreased number of referrals for assessment during March, April and May 2020.

Key stakeholders expressed their appreciation for our collaborative approach, and acknowledged our responsiveness and level of engagement, as well as the quality and relevance of our advice.



**PERFORMANCE  
OBJECTIVE****Shape**

**We provide Australian governments, law enforcement and industry with intelligence and advice to enable better decision-making in relation to security responses, policies and priorities, including warning of emerging and imminent threats.**

**2019–20 RESULT****Achieved**

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

We provided constructive support to government decision-making on border security during the reporting period through our contributions to stakeholders' policy processes, and our advice that enhanced stakeholder decision-making on matters relevant to national security. Our engagement with stakeholders helped increase their understanding of our security assessment processes, which promoted collaboration on visa security assessment issues of mutual interest.

Our advice also positively shaped stakeholder referral criteria through improved awareness of our emerging and priority areas of interest.

We provided additional advice to stakeholders on procedures for recording and processing visa applicants, with security-relevant reporting reducing unnecessary or repeat referrals for security assessment.

**PERFORMANCE  
OBJECTIVE**

**Build**

**2019–20 RESULT**

**Achieved**

**We work with our Australian and international partners to build security and intelligence capabilities.**

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

We worked with stakeholders to build their national security capabilities in visa assessment, and to reduce pressure on these agencies when seeking ASIO guidance on security assessments, in the following ways.

- We worked collaboratively with stakeholders to enhance visa-screening arrangements that were placing considerable pressure on ASIO and partner agencies. This has been a multi-year process to develop stakeholder capability, with agencies progressing towards a more efficient alternative process. In the interim, we have implemented a number of measures to reform the current process, including providing training and advice to stakeholders.
- We continued our successful work with partners in Operation Sovereign Borders to investigate and counter serious threats to Australia's territorial and border integrity. We advised on—and contributed to—Operation Sovereign Borders information requirements, including through our work with community partners.

- Our reporting provided security advice on the impact of changes in government policy and the onset of COVID-19 on community sentiment about the prospects of irregular migration ventures.

Key stakeholder feedback highlighted their appreciation of our collaborative approach in engaging with them, and the relevance of our advice.

## Disrupting people-smuggling activities

In 2019–20 we continued to mitigate serious threats to Australia’s territorial and border integrity by furnishing security assessments to Home Affairs. For example, we investigated an onshore visa applicant whom we assessed to have previously facilitated people-smuggling activities. We concluded that they were directly or indirectly a risk to Australia’s security, and that it would not be consistent with security requirements for them to hold an Australian visa. We subsequently furnished an adverse security assessment to Home Affairs recommending their visa cancellation.

## Key mission 4: protective security advice

### PERFORMANCE OBJECTIVE

### Shape

### 2019–20 RESULT

### Achieved

We provide Australian governments, law enforcement and industry with intelligence and advice to enable better decision-making in relation to security responses, policies and priorities, including warning of emerging and imminent threats.

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

During the reporting period, our physical protective security advice and services continued to inform and shape the protective security approach of national security partners, government bodies and industry. We released another eight security managers guides on our Outreach website—a subscription-based portal disseminating unclassified reporting, and domestic and international security advice. We were also instrumental in helping government and private sector stakeholders deal with physical security-related issues arising from the COVID-19 pandemic. We provided practical advice in updated security managers guides and security equipment guides published on the Outreach website and the GovTEAMS website.

We also provided Technical Surveillance Countermeasures (TSCM) assistance and advice to government agencies. This included TSCM inspections (commonly referred to as ‘sweeps’) of government facilities and other client premises to protect security-classified or sensitive discussions, information and activities from technical compromise. In addition, we provided TSCM assurance to multi-agency missions for new and existing overseas government facilities.

**PERFORMANCE  
OBJECTIVE**

**We work with our Australian and international partners  
to build security and intelligence capabilities.**

## Build

**2019–20 RESULT**

## Achieved

Source: ASIO Corporate Plan 2019–20; addresses ASIO PBS 2019–20

We worked with national security partners throughout 2019–20 to build their protective security capabilities, including in the following ways.

- We held a two-day security zones briefing<sup>3</sup> attended by 144 participants from Australian governments and defence industry. The briefing provided attendees with technical advice on constructing and managing security zones as detailed in the Australian Government Protective Security Policy Framework (PSPF), which helped participants to better protect their people, information and assets.
- We provided capability and advice to help government partners maintain their capability to securely deploy assets to overseas environments. Our assistance focused on environments with high or extreme threat levels, and assets which, if compromised, could cause damage to Australia and its national interests.
- We also continued to conduct Zone 5<sup>4</sup> inspections, issuing a number of certifications for Australia-based facilities requiring **TOP SECRET** information and assets, thereby ensuring sustained access to critical information and systems.

<sup>3</sup> This briefing was held to capture the backlog of interested parties seeking to attend our five-day Security Zones course. The two-day briefing gave an overview of all concepts (in less detail) provided in the five-day course, and highlighted common pitfalls and important information. The briefing was a triage activity, not a replacement for the course.

<sup>4</sup> The Australian Government Protective Security Policy Framework mandates that all Zone 5 facilities in Australia must be certified by ASIO before becoming operational. In some cases, ASIO inspection reports recommend that facility owners introduce additional measures to achieve certification. The difference between the number of inspection reports completed (42) and certifications issued (52) reflects that this work does not align with the same financial year, and that work undertaken by facility owners to implement report recommendations issued in previous years has enabled certification to be issued this financial year.

Table 2: ASIO physical protective security advice and services, 2019–20

		2017–18	2018–19	2019–20 <sup>5</sup>
<b>Physical security certification program</b>				
Zone 5 facilities	Site inspections and reports	89	81	42
	Certifications issued	60	40	52
Courier services	Site inspections and reports	1	8	1
	Endorsements issued	0	8	0
<b>Security products evaluated</b>				
Security products evaluated		71	87	87
<b>Protective security review</b>				
Protective security risk review reports		1	0	1
<b>Communications</b>				
Publications	Protective security circulars	6	1	2
	Security managers guides	10	7	8
	Security equipment guides	4	1	2
	Technical note annexes	0	0	0
Training	Protective security training courses	4	6	4
	Safe maintainer courses	2	1	0
	SCEC <sup>6</sup> -approved locksmith briefings	1	1	2
	SCEC-approved consultant briefings	0	2	0

<sup>5</sup> The downturn in activities requiring travel, meetings and face-to-face interaction (for example, training) was due to physical distancing rules imposed as a consequence of the COVID-19 pandemic.

<sup>6</sup> Security Construction and Equipment Committee

## Analysis of performance

We achieved our purpose during the reporting period through the delivery of three key services: identifying and mitigating efforts to harm Australians and Australia; providing intelligence and advice to enable better decision-making; and building our partners' security and intelligence capabilities.

Some activities were significantly constrained by two factors: the COVID-19 pandemic, and a challenging and rapidly changing technology environment.

COVID-19 required an immediate response by ASIO across the breadth of our work. We adapted operational practices to provide security advice to government on attempts to target Australia and its interests, including by individuals using the crisis to their advantage. Although some of our activities were significantly affected owing to the travel restrictions, we continued to analyse and identify potential threats.

We continue to be challenged by rapidly evolving technological advancements. These include the widespread adoption of new technology, including encryption and anonymising technologies, by those seeking to threaten Australia's security. The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* has gone some way to address these challenges by contemporising our access to security-relevant data. We took advantage of these new powers within 10 days of the legislation coming into effect; a clear indication of its significance to our mission.

Separately, we assess that the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* has hardened Australia's security environment, with our adversaries adjusting their behaviour in response to its introduction. We recognise we have been entrusted with significant powers under this and existing legislation; our application of these powers will continue to be lawful, ethical and proportionate to the security threat or matter at hand.

Finally, our partnerships have contributed significantly to the achievement of our purpose. Our ability to leverage existing and new partnerships with domestic, international and industry partners enabled access to new information sources and enhanced capability. Continuing to bolster our relationships will be critical to our future success.

# Report on financial performance

## Financial performance

The COVID-19 pandemic impacted the delivery of ASIO's activities for the 2019–20 financial year, resulting in less expenditure than initially planned. The financial result—excluding depreciation and amortisation—was a surplus of \$17.1 million, which represents 3.4 per cent of budget. The previous financial year result was a deficit of \$14.4 million after a significant adjustment for provisions and an overspend in supplier costs.

Included in ASIO's 2019–20 operating budget was \$29.9 million for ongoing planning and design work relating to enterprise transformation. Given the challenge of progressing with this program through the uncertain COVID-19 economic environment, a more modest program of reforms, based on similar organisational priorities, will start to be progressed in 2020–21. ASIO also received \$28.6 million to sustain specific existing operations.

ASIO's 2019–20 Departmental Capital Budget funding was \$61.3 million, compared with \$83.5 million the previous financial year. This funding has been applied to the necessary development, enhancement and replacement of assets to support ASIO's operational effectiveness in the increasingly fluid security and technology environments. In 2019–20 ASIO received \$10.9 million as an equity injection, compared with \$5.4 million in 2018–19.

ASIO has continued to identify and implement efficiencies across its operations and contribute to Australian Government savings measures. Further consideration will be given during the 2020–21 financial year to the sustainability of ASIO's operations, given the challenges and opportunities presented by the future operating environment.

A table summarising ASIO's total resources for 2019–20 is provided at **Appendix A**. Our total expenses by outcome for this reporting period are at **Appendix B**.





# 5

## **Management and accountability**

---

# At a glance

p. 59

In response to COVID-19, ASIO adapted its operating model to maintain coverage of high-priority targets related to our counter-terrorism and counter-espionage and foreign interference missions.

p. 63

Ethical behaviour and integrity are core values of the Organisation.

# Corporate governance

Our governance processes guide us in achieving our mission and meeting public expectations of probity, accountability and transparency.

The Director-General of Security is the accountable authority for ASIO under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

During the reporting period, we introduced a new governance framework to establish clearer points of accountability and streamline decision-making processes. The new structure consists of an Executive Committee, supported by two advisory committees (the Security and Compliance Committee, and the Capability and Investment Committee) and an independent advisory committee (the Audit and Risk Committee).

## ASIO governance framework



## Executive Committee

The Executive Committee, chaired by the Director-General, is ASIO's peak governing body. It provides executive oversight of all ASIO activities, including:

- setting the strategic direction for the Organisation;
- setting priorities, and reviewing and assessing performance; and
- managing enterprise risks.

The Executive Committee receives regular reporting from supporting advisory committees on matters including developments in the security environment, capability development and management, performance and risk management, and diversity and inclusion goals.

## Security and Compliance Committee

The Security and Compliance Committee, chaired by the Deputy Director-General Intelligence Service Delivery, advises the Executive Committee on security and compliance matters.

## Capability and Investment Committee

The Capability and Investment Committee, chaired by the Deputy Director-General Enterprise Service Delivery, advises the Executive Committee on Organisational capability and investment. Capability refers to the capacity, materials and expertise to perform the necessary functions of the Organisation, including people, finance, technology, systems and property.

# ASIO's response to COVID-19

## Steps taken

In response to COVID-19, ASIO adapted its operating model to maintain coverage of high-priority targets related to our counter-terrorism and counter-espionage and foreign interference missions. ASIO reprioritised its production of intelligence advice, with a focus on national security threats impacted by COVID-19 pandemic responses, and provided assessments in response to emerging customer demand.

In March 2020 we mobilised our COVID-19 Crisis Management Team (CMT). The CMT manages our Organisation-wide posture to the pandemic to mitigate potential impacts on our people and daily operations, and coordinates our contribution to whole-of-government COVID responses.

To reduce the risk of COVID-19 infection within ASIO and the broader community, our staff working in Canberra, the regions and overseas quickly commenced modified working arrangements. Each of our sites and offices continue to monitor local conditions, and have in place appropriately calibrated contingency planning procedures to maintain workforce safety and business continuity.

Minimising disruption to our daily operations has been another CMT priority. We have activated business continuity plans to support our workflows and avert any disruption to our core systems and key services. Because of security challenges, our daily workflows cannot easily be done remotely, but the pandemic has provided fresh impetus to existing programs that test our ability to work beyond the office.

## Our partnerships

Nothing we do is done in isolation, so our partnerships within the Australian community, the private sector, and members of the intelligence community and law enforcement—in Australia and overseas—have been vital. By leveraging our partnership networks, we were able to enhance our understanding of competing priorities and local and international stakeholder positions.

During the COVID-19 pandemic, we explored new ways to manage our partnerships within the constraints of new workplace measures. This ranged from proactively supporting our public and private sector stakeholders to manage the additional security challenges brought about by the pandemic, to providing tailored technical working-from-home advice.

## Outlook

The challenges presented by COVID-19 are fluid. We continue to closely monitor the COVID-19 situation in Australia and overseas, assess potential risks to our workflows, and develop mitigation strategies to ensure business continuity. As situations evolve nationally and worldwide, we will continue to assess and update our response.

## External scrutiny

### Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) performs a key role in the independent oversight and accountability framework by providing assurance to the Australian community about ASIO's performance of its functions.

The PJCIS remit includes overseeing ASIO's administration and expenditure; reviewing national security bills; and ensuring national security legislation remains necessary, proportionate and effective.

In 2019–20, ASIO provided written submissions to the PJCIS Review of Administration and Expenditure No. 18 (2018–19). During 2019–20, ASIO also contributed, either directly or through consultation with Home Affairs, to a number of other PJCIS inquiries, including:

- inquiries on the listing and relisting of terrorist organisations;
- the review of the Counter-Terrorism Legislation Amendment (2019 Measures No. 1) Bill 2019;
- the review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018*;
- the review of the Australian Citizenship Amendment (Citizenship Cessation) Bill 2019;
- the review of the renunciation by conduct and cessation provisions in the *Australian Citizenship Act 2007*;
- the ongoing review into the mandatory data retention regime;
- the review of the ASIO Amendment Bill 2020;
- the inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press;
- the review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020; and
- the review of the Identity-matching Services Bill 2019.

### Other parliamentary committee inquiries

ASIO provides submissions to other parliamentary committees as appropriate. In 2019–20, ASIO contributed, either directly or through consultation with Home Affairs, to:

- the Senate Environment and Communications Committee's inquiry into press freedom;
- the Senate Select Committee on Foreign Interference through Social Media;
- the Senate Standing Committee on Finance and Public Administration's Review of the Intelligence and Security Legislation Amendment (Implementing Independent Intelligence Review) Bill 2020; and
- the Joint Standing Committee on Electoral Matters inquiry into the 2019 federal election.

## Senate Legal and Constitutional Affairs Committee

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate estimates process on 2 March 2020. ASIO's evidence to the committee can be found in the estimates' Hansard for those days (refer to [www.aph.gov.au/Parliamentary\\_Business/Senate\\_Estimates](http://www.aph.gov.au/Parliamentary_Business/Senate_Estimates) and navigate to the relevant hearing).

## Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) assists ministers to oversee and review the activities of intelligence agencies for legality and propriety.

The IGIS performs this function through inspections, inquiries and investigations into complaints. The Inspector-General is also required to assist the government to assure the public and the parliament that Commonwealth intelligence and security matters are open to scrutiny. The IGIS retains statutory powers akin to those of a standing royal commission.

Meeting our legal obligations and embodying the highest ethical standards is critical to maintaining the trust of the Australian public and our ongoing effectiveness as Australia's security intelligence organisation.

Every ASIO officer is responsible for complying with our legislated requirements, the Minister's Guidelines for ASIO, and associated internal policies and procedures. Central to this is acting with integrity and ensuring proportionality in all our work.

During 2019–20 the IGIS regularly inspected activities across our operational functions, and investigated a small number of complaints received by the Office. In the 2019–20 reporting period, the Office of the IGIS finalised and made recommendations on three inquiries, the results of which were reported to the ASIO Audit and Risk Committee for review. ASIO accepted all inquiry recommendations and is at various stages of implementation in consultation with the Office of the IGIS and relevant agencies. We are committed to acting with legality and propriety, and in 2019–20 we acted comprehensively and systematically to address issues the IGIS identified as requiring improvement.

During the reporting period, we continued to support the IGIS's important work by proactively briefing IGIS staff on a number of operational matters, including new capabilities and initiatives.

## Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor (INSLM) reviews the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, and reports to the Prime Minister and parliament on an ongoing basis.

The INSLM considers whether the laws contain appropriate safeguards to protect individuals' rights, remain proportionate to threats of terrorism or national security, and remain necessary. The Prime Minister may also refer a counter-terrorism or national security matter to the INSLM, either at the INSLM's suggestion or on the Prime Minister's initiative, under the Act.

During 2019–20, ASIO provided submissions to the INSLM's review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018*.

## Independent Reviewer of Adverse Security Assessments

The Independent Reviewer of Adverse Security Assessments reviews ASIO assessments which negatively impact on certain individuals (refer to **Appendix I** for eligibility criteria) who are in immigration detention and seeking an Australian visa. The Independent Reviewer conducts an initial primary review of each adverse security assessment, followed by reviews every 12 months for the duration of the adverse assessment.

In conducting reviews, the Independent Reviewer examines all ASIO material relied on in making the adverse assessment, as well as any other relevant material. This may include submissions or representations made by the applicant.

The Independent Reviewer also considers the overall security environment, informed by ASIO's assessment of security threats, and any changes to the applicant's circumstances or ideology during their time in detention.

**Appendix I** provides the Independent Reviewer's annual report for the current reporting period.



# Compliance

Ethical behaviour and integrity are core values of the Organisation, and are essential to sustain the confidence and trust of the parliament and the Australian people. We earn this confidence through strict compliance with the law, stringent application of policies and procedures, and active cooperation with external oversight bodies.

Centralised internal audit and compliance functions are key components of ASIO's approach to corporate governance. These provide assurance to the Director-General that our risk, control and compliance measures ensure our resources are used efficiently, effectively and ethically. This includes taking all reasonable steps to prevent, deter and address fraud. These efforts also serve to ensure ASIO is positioned to meet current and future security challenges.

## Internal audit function

ASIO's internal audit function is designed to add value and improve our operations and service delivery. By applying a systematic and disciplined approach to evaluation and advice, the function supports effective and efficient internal control and governance frameworks.

Subject to security policies and operational considerations, our internal audit function has unrestricted access to all ASIO premises, work areas, documentation and information necessary to meet its responsibilities.

During the reporting period, ASIO undertook a program of compliance audits and performance reviews.

## Compliance function

ASIO's compliance function is focused on ensuring the Organisation continues to demonstrate our commitment to the highest standards of ethics and compliance with all applicable laws, regulations, rules and policies.

During the reporting period, we continued to mature internal assurance frameworks, including establishing a centralised compliance function. This created a formal and structured Organisation-wide mechanism to improve and monitor our compliance and assurance practices.

## ASIO Audit and Risk Committee

The ASIO Audit and Risk Committee is an independent advisory body, responsible for providing independent assurance and advice to the Director-General and the Executive Committee on ASIO's risk oversight and management, financial and performance reporting responsibilities, and internal control systems.

The committee operates under a charter which sets out its functions and responsibilities in accordance with section 45 of the PGPA Act and section 17 of the Public Governance Performance and Accountability Rule.<sup>7</sup>

<sup>7</sup> In accordance with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the annual report has not provided a direct electronic address for the charter determining the function of the ASIO Audit and Risk Committee.

Under the Audit and Risk Committee's charter, the committee has four external members, including an external chair as well as observers from the Australian National Audit Office.<sup>8</sup> The audit committee members have a broad range of appropriate qualifications, knowledge, skills and experience relevant to ASIO's operations. This includes at least one member with accounting or related financial management experience, with an understanding of accounting and auditing standards in a public sector environment. On appointment, committee members receive an induction briefing on ASIO governance and operations.

During this reporting period, the committee met five times (four quarterly meetings and an extraordinary meeting convened for the Financial Statements review). Each meeting had a quorum, with all members attending two meetings, and all but one attending the remaining three.

## Fraud control and management

ASIO has zero tolerance for fraudulent behaviour. ASIO treats both suspected and actual fraud seriously and takes all reasonable steps to prevent, detect and deal with fraudulent behaviour. The *ASIO Fraud Control Plan 2019–21* documents our approach to fraud awareness, prevention, detection, reporting and investigation, and our commitment to ensuring efficient, effective and ethical use of resources—including the information and data we collect as well as the resources received

from government. Our fraud prevention measures are in line with the Commonwealth Fraud Control Framework.

During the reporting period, we conducted a fraud risk assessment and reviewed the *ASIO Fraud Control Plan 2019–21* to address identified risks. As part of this framework, all staff must complete mandatory eLearning on ethics and accountability, including modules on fraud, every three years.

The *ASIO Fraud Strategy Statement 2019–21* ([www.asio.gov.au/asio-fraud-strategy-statement.html](http://www.asio.gov.au/asio-fraud-strategy-statement.html)) provides further information on our fraud control and management arrangements.

<sup>8</sup> In accordance with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the annual report has not provided membership and remuneration details.

# Significant legal matters affecting ASIO's business

ASIO continued to be involved in numerous legal proceedings in courts, tribunals and other forums. Matters included terrorism prosecutions; judicial and merits reviews of security assessments; and civil lawsuits.

## Administrative Appeals Tribunal

The Administrative Appeals Tribunal (AAT) reviewed a number of security assessments in the 2019–20 reporting period, most of which involved review of personnel security assessments.

Separately, three current and former ASIO employees brought review proceedings challenging Comcare decisions. AAT decisions are reported on the Australasian Legal Information Institute (AustLII) website, [www.austlii.edu.au](http://www.austlii.edu.au).

## Tribunal reviews—security assessments

Over the 2019–20 reporting period, ASIO managed 13 adverse security assessment reviews before the AAT, including those relating to cancelled or refused passports, visas and security clearances.

Of these 13 matters:

- three decisions were handed down, affirming the adverse security assessment which was the subject of the review;
- three assessments were remitted to ASIO for new assessments to be prepared, which resulted in the issuing of three non-prejudicial assessments in this reporting period;
- one matter was heard, with the decision remaining reserved at the end of this reporting period; and
- six matters were pending at the end of this reporting period.

## Tribunal reviews—archives matters

Over this reporting period, we managed two AAT reviews of National Archives matters.

## Criminal prosecutions

In collaboration with our law enforcement partners and prosecuting authorities—and with appropriate protections—we provided information for use as evidence to prosecutions, and responded to subpoenas and disclosure requests.

## Federal and High Court reviews—security assessments

ASIO was involved in Federal and High Court proceedings, both as a respondent in security assessment reviews and as an interested third party in other proceedings. We worked closely with other stakeholders to manage the collective Commonwealth interest.

# Management of human resources

## Current workplace agreement

ASIO's terms and conditions of employment are set out in a determination approved by the Director-General under the ASIO Act.

Formal negotiations for ASIO's 11th Workplace Agreement concluded in March 2020, with 91.5 per cent of employees voting in favour of the new determination, which took effect from 2 April 2020. Consistent with Australian Government policy, ASIO paused the implementation of the initial pay rise for six months to allow the circumstances surrounding COVID-19 to become clearer.

## Performance management

ASIO continued to refine its performance framework through the reporting year and achieved greater alignment with the business planning process. This was supported by workshops for team deliverables and objectives. All ASIO staff required to participate in the performance cycle did so in 2019–20.

Our early intervention initiatives continue to assist line managers and employees to address performance issues and further strengthen the high performance culture.

## People strategy

A focus over the past year has been to mature our workforce analytics capability to enable strategic workforce management. The development of an enterprise data warehouse has enabled the delivery of automated real-time workforce reports to support strategic workforce-related decision-making. This has also enabled line managers to use self-service dashboard reporting to support their day-to-day considerations.

## Diversity and inclusion

ASIO has made significant progress towards increasing the diversity of its workforce and ensuring the workplace is inclusive. Guided by our Diversity and Inclusion Strategy 2018–20, progress has been overseen by ASIO's Diversity and Inclusion Council and supported by ASIO's diversity champions and networks.

While COVID-19 restrictions affected some of the planned diversity and inclusion awareness-raising initiatives, the Organisation made significant progress during the year, including:

- launching the ASIO Innovate Reconciliation Action Plan (RAP) endorsed by Reconciliation Australia;
- achieving silver accreditation in the Australian Workplace Equality Index—Australia’s national benchmarking instrument for gender and sexually diverse workplace inclusion—for the second consecutive year. As part of our submission, we demonstrated improvements in visibility, training and inclusive human resources policies to help ensure best practice as an employer of choice for gender-diverse and sexually diverse people. ASIO ranked fourth among participating federal government agencies;
- improving gender balance in general entry-level programs; and
- establishing a new staff-led network focused on parents.

ASIO’s progress can be seen in the results of an all-staff survey conducted in March 2020 where 90 per cent of staff reported diversity and inclusion was valued by the Organisation; an increase of 11 per cent from the previous survey. The staff survey also showed that most women reported high engagement and positive intentions to remain with ASIO. The survey confirmed support at all levels for the Organisation’s ‘if not, why not’ approach to flexible working.

## Diversity networks

ASIO has seven staff-led networks which are an essential part of creating a diverse and inclusive culture. The networks provide support to staff and empower them to initiate organisational change to achieve ASIO’s diversity and inclusion goals. Senior Executive Service sponsorship ensures that issues of particular concern to a network can be deliberated at senior levels within the Organisation.

Statistics on the diversity of our workforce are provided at **Appendix E**.

## ASIO Ombudsman

The ASIO Ombudsman is an external service provider who works to resolve employee issues or concerns—both impartially and informally—through advice, consultation and mediation.

During the reporting year, the ASIO Ombudsman provided support and advice to employees and line managers, including in response to contacts from employees; and undertook one preliminary review of investigative matters.

## Asset management

The Ben Chifley Building continued to support the business and capability needs of ASIO and its partners. Our corporate suites, including Australia’s largest security-accredited auditorium, hosted a range of events over 2019–20 before the introduction of COVID-19 restrictions.

## Purchasing

Throughout 2019–20 we adhered to the Commonwealth Procurement Rules (CPR) and associated policy and guidelines. Our compliance was monitored through our Audit and Risk Committee. No significant issues were identified, and overall compliance was acceptable.

## Consultants

We entered into 27 new consultancy contracts involving total actual expenditure of \$4 714 610 (Goods and Services Tax (GST)–inclusive). In addition, five ongoing consultancy contracts were active during the period, involving total actual expenditure of \$885 631 (GST-inclusive).

Table 3: ASIO contract and consultant data

	Total
Number of new contracts entered into during the period	27
Total actual expenditure on new contracts during the period (inc. GST)	\$4 714 610
Number of ongoing contracts engaging consultants which were entered into during the previous period	5
Total actual expenditure on ongoing contracts during the period (inc. GST)	\$885 631

We applied the CPR and Department of Finance guidance when selecting and engaging consultants. We also followed internal policy and associated procedures on identifying and determining the nature of a contract. This ensured that we used appropriate methods for engaging and contracting consultants.

We engaged consultants when we needed professional, independent and expert advice or services that were not available from within the Organisation.

Annual reports contain information about actual expenditure on contracts for consultancies; information on the value of contracts and consultancies is available on the AusTender website. However, we are not required to publish information on the AusTender website, in line with authorised exemptions to avoid prejudice to our national security activities. A list of consultancy contracts to the value of

\$10 000 or more during this reporting period, and the total value of each of those contracts over the life of each contract, is available on request to the PJCIS, which oversees our administration and expenditure.

## Australian National Audit Office access clauses

During this reporting period, we did not enter into any contracts valued at \$100 000 or more that did not provide the Auditor-General with access to the contractor’s premises.

## Exempt contracts

The Director-General has applied measures necessary to protect national security which exempt ASIO from publishing details of contract arrangements, including standing offers,

in accordance with clause 2.6 of the CPR. Details of our arrangements, contracts and standing offers are available on request to the PJCIS.

## Procurement initiatives to support small business

Throughout 2019–20 we adhered to the CPR and associated policy and guidelines. Our compliance was monitored through our Audit and Risk Committee. No significant issues were identified, and overall compliance was acceptable.

ASIO supports small business participation in the Australian Government procurement market. Small and medium enterprises (SME) and small enterprise participation statistics are available on the Department of Finance's website.

Our procurement practices to support SME include:

- standardising contracts and approach-to-market templates, using clear and simple language;
- ensuring information is easily accessible through the electronic advertisement of business opportunities and electronic submission for responses; and
- using electronic systems to facilitate the Department of Finance's Procurement On-Time Payment Policy for Small Business, including payment cards.

We recognise the importance of ensuring that small businesses are paid on time. Statistics on SME's participation in Commonwealth Government procurement are available on the Department of Finance's website at <https://finance.gov.au/government/procurement/statistics-australian-government-procurement-contracts>.

This incorporates our annual reporting requirements for Public Governance, Performance and Accountability Rule 2014—17AG 'Information on management and accountability'.



## Other mandatory information

### Advertising and market research

In the financial year 2019–20, ASIO expended \$313 025 on marketing and advertising for recruitment activities and campaigns. Further information on these advertising campaigns is available at [www.asio.gov.au](http://www.asio.gov.au) and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website (see also **Appendix G**).

ASIO does not fall within the definition of agencies covered by the reporting requirements of section 311A of the *Commonwealth Electoral Act 1918*.

### Disability reporting

Since 1994, non-corporate Australian Government entities have reported on their performance as policy advisers, purchasers, employers, regulators and providers under the Commonwealth Disability Strategy. In 2007–08, reporting on the employer role was transferred to the Australian Public Service Commission's *State of the service* reports and the *APS Statistical Bulletin*. These reports are available at [www.apsc.gov.au](http://www.apsc.gov.au). Since 2010–11, entities have not been required to report on these functions.

The Commonwealth Disability Strategy has been replaced by the National Disability Strategy 2010–20, which sets out a 10-year national policy framework to improve the lives of people with a disability, promote participation, and create a more inclusive society. It acts to ensure the principles underpinning the United Nations Convention on the Rights of Persons with Disabilities are incorporated into Australia's policies and programs that affect people with disability, their families and carers.

All levels of government will continue to be held accountable for the implementation of the strategy through biennial progress reporting to the Council of Australian Governments. Progress reports can be found at [www.dss.gov.au](http://www.dss.gov.au). Disability reporting is included in the Australian Public Service Commission's *State of the service* reports and the *APS Statistical Bulletin*. These reports are available at [www.apsc.gov.au](http://www.apsc.gov.au).

**Appendix E** provides information on the diversity of our workforce, including statistics on people with a disability.

# Information required by another Act or instrument

## Archives Act 1983

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to the release of records under the *Archives Act 1983*, which allows public access to Commonwealth records in the ‘open period’. In accordance with changes to the Archives Act in 2010, the open period is transitioning from 30 to 20 years, and currently covers all Commonwealth records created before 2000. ASIO works closely with the National Archives of Australia to facilitate access to ASIO records, while balancing various and sometimes competing priorities.

In 2019–20, ASIO received 334 applications for access to ASIO records and completed a total of 399 requests, equating to 72 820 pages. A total of 59 per cent of requests were completed within the 90-day legislative time frame. The small reduction in requests completed in the reporting period is due to the complexity of assessments, and an increase in the completion of longstanding cases, in addition to new requests. Further, the way we conduct some of our routine assessments was affected by COVID-19 restrictions; COVID-19 also had an impact on our resourcing during the latter half of the reporting period.

Table 4: Access to ASIO records

	2017–18	2018–19	2019–20
Applications for record access	345	344	334
Requests completed	310	410	399
Pages assessed	36 312	57 783	72 820
Percentage of requests completed within 90 days	66.7%	60%	59%

## Australian Security Intelligence Organisation Act 1979

Section 94 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) requires that ASIO's annual report include statements on the Organisation's questioning warrants and questioning and detention warrants, special intelligence operation authorisations, and telecommunications data access authorisations.

The statement on questioning warrants and questioning and detention warrants is provided at **Appendix J**. To ensure compliance with the determination made by the Minister for Finance under section 105D of the PGPA Act, and to avoid prejudice to ASIO's activities, **Appendix K** relating to special intelligence operation authorities, **Appendix L** relating to telecommunications data access authorisations, **Appendix M** relating to use of technical assistance requests, technical assistance notices and technical capability notices and **Appendix N** relating to use of special powers under warrant have been removed from the annual report tabled in parliament.

These classified appendices will be separately provided to ASIO's minister and, as required by the ASIO Act, to the Leader of the Opposition. Copies of the classified appendices will also be provided to the Attorney-General, the IGIS, and the INSLM. **Appendix L** relating to telecommunications data access authorisations will also be provided to the PJCIS.

## Work Health and Safety Act 2011

Schedule 2, Part 4 of the *Work Health and Safety Act 2011* requires non-corporate Commonwealth entities to include in their annual report information on health and safety outcomes and initiatives taken during the reporting period to ensure the health, safety and welfare of workers who carry out work for them.

Our report for 2019–20 is provided at **Appendix F**.

## Commonwealth Electoral Act 1918—advertising and market research

Section 311A of the *Commonwealth Electoral Act 1918* requires annual reporting by each Commonwealth department on amounts paid by, or on behalf of, the Commonwealth department for advertising and market research.

Our report for 2019–20 is provided at **Appendix G**.

## Environment Protection and Biodiversity Conservation Act 1999

Section 516A of the *Environment Protection and Biodiversity Conservation Act 1999* requires Commonwealth entities to report on how the activities of the entity during the period accorded with the principles of ecologically sustainable development.

Our report for 2019–20 is provided at **Appendix H**.





F

**Financial  
statements**





## CONTENTS

INDEPENDENT AUDITOR'S REPORT	79
STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY	81
STATEMENT OF COMPREHENSIVE INCOME	83
STATEMENT OF FINANCIAL POSITION	84
STATEMENT OF CHANGES IN EQUITY	86
STATEMENT OF CASH FLOWS	87
NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS	89
Overview	89
<b>1. Financial performance</b>	<b>92</b>
1.1 EXPENSES	92
1.2 OWN-SOURCE REVENUE AND GAINS	93
<b>2. Financial position</b>	<b>94</b>
2.1 FINANCIAL ASSETS	94
2.2 NON-FINANCIAL ASSETS	95
2.3 PAYABLES	98
2.4 INTEREST BEARING LIABILITIES	98
2.5 PROVISIONS	98
<b>3. Funding</b>	<b>100</b>
3.1 APPROPRIATIONS	100
<b>4. Managing uncertainties</b>	<b>102</b>
4.1 CONTINGENT ASSETS AND LIABILITIES	102
4.2 FINANCIAL INSTRUMENTS	102
<b>5. Other information</b>	<b>104</b>
5.1 KEY MANAGEMENT PERSONNEL REMUNERATION	104
5.2 RELATED PARTY DISCLOSURES	104
5.3 MAJOR BUDGET VARIANCES	105

Due to rounding, figures presented throughout these financial statements may not add precisely to the totals provided.







## INDEPENDENT AUDITOR'S REPORT

### To the Minister for Home Affairs

#### Opinion

In my opinion, the financial statements of the Australian Security Intelligence Organisation (the Entity) for the year ended 30 June 2020:

(a) comply with:

- Australian Accounting Standards – Reduced Disclosure Requirements; and
- the requirements *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*

as amended by section 105 D of the *Public Governance, Performance and Accountability Act 2013*.

(b) present fairly the financial position of the Entity as at 30 June 2020 and its financial performance and cash flows for the year then ended in accordance with the requirements of section 105 D of the *Public Governance, Performance and Accountability Act 2013*.

The financial statements of the Entity, which I have audited, comprise the following as at 30 June 2020 and for the year then ended:

- Statement by the Director-General of Security;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Cash Flow Statement; and
- Notes to the financial statements, comprising a summary of significant accounting policies and other explanatory information.

#### Basis for opinion

I conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the Entity in accordance with the relevant ethical requirements for financial statement audits conducted by the Auditor-General and his delegates. These include the relevant independence requirements of the Accounting Professional and Ethical Standards Board's APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* (the Code) to the extent that they are not in conflict with the *Auditor-General Act 1997*. I have also fulfilled my other responsibilities in accordance with the Code. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

#### Accountable Authority's responsibility for the financial statements

As the Accountable Authority of the Entity, the Director-General of Security is responsible under the *Public Governance, Performance and Accountability Act 2013* (the Act) for the preparation and fair presentation of annual financial statements that comply with Australian Accounting Standards – Reduced Disclosure Requirements and the rules made under the Act. The Director-General of Security is also responsible for such internal control as the Director-General of Security determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

GPO Box 707 CANBERRA ACT 2601  
38 Sydney Avenue FORREST ACT 2603  
Phone (02) 6203 7300 Fax (02) 6203 7777

In preparing the financial statements, the Director-General of Security is responsible for assessing the ability of the Entity to continue as a going concern, taking into account whether the Entity's operations will cease as a result of an administrative restructure or for any other reason. The Director-General of Security is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the assessment indicates that it is not appropriate.

### **Auditor's responsibilities for the audit of the financial statements**

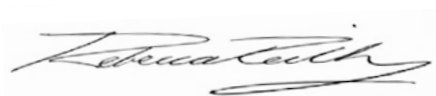
My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with the Australian National Audit Office Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

As part of an audit in accordance with the Australian National Audit Office Auditing Standards, I exercise professional judgement and maintain professional scepticism throughout the audit. I also:

- identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control;
- obtain an understanding of internal control relevant to the audit 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 Entity's internal control;
- evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Director-General of Security;
- conclude on the appropriateness of the Director-General of Security's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Entity's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the Entity to cease to continue as a going concern; and
- evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with the Director-General of Security regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Australian National Audit Office



Rebecca Reilly  
Executive Director

Delegate of the Auditor-General

Canberra  
6 August 2020

## STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2020 comply with subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and are based on properly maintained financial records as per subsection 41(2) of the PGPA Act.

In my opinion, at the date of this statement, there are reasonable grounds to believe that ASIO will be able to pay its debts as and when they fall due.

A handwritten signature in black ink, appearing to read 'Mike Burgess', is positioned above the printed name and title.

**Mike Burgess**

Director-General of Security

6 August 2020



## STATEMENT OF COMPREHENSIVE INCOME

### for the period ended 30 June 2020

	Notes	2020 \$'000	Original budget 2020 \$'000	2019 \$'000
<b>EXPENSES</b>				
Employee benefits	1.1.A	287 088	275 842	272 077
Suppliers	1.1.B	151 999	211 609	198 646
Depreciation and amortisation	2.2.A	139 109	91 931	104 066
Finance costs	1.1.C	8688	-	739
Write-down and impairment of other assets	1.1.D	425	-	656
<b>TOTAL EXPENSES</b>		<b>587 309</b>	<b>579 382</b>	<b>576 184</b>
<b>OWN-SOURCE INCOME</b>				
<b>Revenue</b>				
Sale of services	1.2.A	18 019	21 899	15 147
Other revenue	1.2.B	6141	1772	7300
<b>Gains</b>		<b>61</b>	<b>145</b>	<b>25</b>
<b>TOTAL OWN-SOURCE INCOME</b>		<b>24 221</b>	<b>23 816</b>	<b>22 473</b>
<b>Net cost of services</b>		<b>(563 087)</b>	<b>(555 566)</b>	<b>(553 711)</b>
<b>REVENUE FROM GOVERNMENT</b>	3.1	<b>473 011</b>	<b>463 635</b>	<b>435 196</b>
<b>DEFICIT ON CONTINUING OPERATIONS</b>	3.1.C	<b>(90 077)</b>	<b>(91 931)</b>	<b>(118 515)</b>
<b>OTHER COMPREHENSIVE INCOME</b>				
Changes in asset revaluation surplus		20 516	-	-
<b>TOTAL COMPREHENSIVE LOSS</b>		<b>(69 561)</b>	<b>(91 931)</b>	<b>(118 515)</b>

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

# STATEMENT OF FINANCIAL POSITION

as at 30 June 2020

		2020	Original budget 2020	2019
	Notes	\$'000	\$'000	\$'000
<b>ASSETS</b>				
<b>Financial assets</b>				
Cash and cash equivalents	2.1.A	16 260	24 749	23 517
Trade and other receivables	2.1.B	110 029	64 198	85 894
Accrued revenue		602	847	575
Amortisation of subleased right-of-use assets income	2.1.C	1441	-	-
<b>Total financial assets</b>		<b>128 332</b>	<b>89 794</b>	<b>109 986</b>
<b>Non-financial assets</b>				
Prepayments		34 748	27 483	26 969
Land and buildings	2.2.A	736 228	136 518	145 865
Property, plant, equipment and computer software	2.2.A	213 740	208 888	194 196
<b>Total non-financial assets</b>		<b>984 717</b>	<b>372 889</b>	<b>367 029</b>
<b>TOTAL ASSETS</b>		<b>1 113 049</b>	<b>462 683</b>	<b>477 015</b>
<b>LIABILITIES</b>				
<b>Payables</b>				
Suppliers	2.3.A	9991	24 681	9373
Other payables	2.3.B	12 420	2366	26 637
<b>Total payables</b>		<b>22 411</b>	<b>27 047</b>	<b>36 010</b>
<b>Interest bearing liabilities</b>				
Leases	2.4.A	618 532	-	-
<b>Total interest bearing liabilities</b>		<b>618 532</b>	<b>-</b>	<b>-</b>
<b>Provisions</b>				
Employee provisions	2.5.A	96 545	81 721	91 336
Restoration obligations	2.5.B	7225	4920	6794
<b>Total provisions</b>		<b>103 770</b>	<b>86 641</b>	<b>98 130</b>
<b>TOTAL LIABILITIES</b>		<b>744 713</b>	<b>113 688</b>	<b>134 140</b>
<b>NET ASSETS</b>		<b>368 336</b>	<b>348 995</b>	<b>342 875</b>

## STATEMENT OF FINANCIAL POSITION

### as at 30 June 2020 (continued)

	Notes	2020 \$'000	Original budget 2020 \$'000	2019 \$'000
<b>EQUITY</b>				
<b>Parent equity interest</b>				
Contributed equity		915 296	913 570	843 097
Reserves		90 374	69 857	69 858
Accumulated deficit		(637 334)	(634 432)	(570 080)
<b>TOTAL EQUITY</b>		<b>368 336</b>	<b>348 995</b>	<b>342 875</b>

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

## STATEMENT OF CHANGES IN EQUITY

### for the period ended 30 June 2020

	2020 \$'000	Original budget 2020 \$'000	2019 \$'000
<b>RETAINED EARNINGS</b>			
Opening balance	(570 080)	(542 501)	(451 565)
Adjustment on initial application of AASB16	22 823	-	-
<b>Comprehensive income</b>			
Deficit for the period	(90 077)	(91 931)	(118 515)
<b>Closing balance</b>	<b>(637 334)</b>	<b>(634 432)</b>	<b>(570 080)</b>
<b>ASSET REVALUATION RESERVE</b>			
Opening balance	69 858	69 857	69 858
<b>Other comprehensive income</b>			
Changes in asset revaluation surplus	20 516	-	-
<b>Closing balance</b>	<b>90 374</b>	<b>69 857</b>	<b>69 858</b>
<b>CONTRIBUTED EQUITY</b>			
Opening balance	843 097	843 097	752 158
<b>Transactions with owners</b>			
<b>Contributions by owners</b>			
Equity injection—appropriation	10 870	8831	5367
Departmental capital budget	61 329	61 642	85 572
<b>Closing balance</b>	<b>915 296</b>	<b>913 570</b>	<b>843 097</b>
<b>CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT</b>	<b>368 336</b>	<b>348 995</b>	<b>342 875</b>

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

#### Accounting policy

##### 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.



## STATEMENT OF CASH FLOWS

### for the period ended 30 June 2020

	Notes	2020 \$'000	Original budget 2020 \$'000	2019 \$'000
<b>OPERATING ACTIVITIES</b>				
<b>Cash received</b>				
Appropriations		473 967	469 762	461 812
Sales of services		18 452	20 267	18 063
Net GST received		23 884	23 641	25 404
Other		5533	1724	7155
<b>Total cash received</b>		<b>521 836</b>	<b>515 394</b>	<b>512 434</b>
<b>Cash used</b>				
Employees		273 653	274 856	260 102
Suppliers		183 282	213 819	217 985
Interest payments on lease liabilities		8414	-	-
Section 74 receipts		31 331	23 671	43 188
Other		-	192	-
<b>Total cash used</b>		<b>496 680</b>	<b>512 538</b>	<b>521 275</b>
<b>NET CASH FROM/(USED BY) OPERATING ACTIVITIES</b>		<b>25 156</b>	<b>2856</b>	<b>(8841)</b>
<b>INVESTING ACTIVITIES</b>				
<b>Cash received</b>				
Proceeds from property, plant, equipment and computer software		641	-	709
<b>Total cash received</b>		<b>641</b>	<b>-</b>	<b>709</b>
<b>Cash used</b>				
Purchase of property, plant, equipment and computer software		79 404	71 049	79 240
<b>Total cash used</b>		<b>79 404</b>	<b>71 049</b>	<b>79 240</b>
<b>NET CASH FROM/(USED BY) INVESTING ACTIVITIES</b>		<b>(78 763)</b>	<b>(71 049)</b>	<b>(78 530)</b>

## STATEMENT OF CASH FLOWS

### for the period ended 30 June 2020 (continued)

	Notes	2020 \$'000	Original budget 2020 \$'000	2019 \$'000
<b>FINANCING ACTIVITIES</b>				
<b>Cash received</b>				
Contributed equity		78 179	70 473	87 337
<b>Total cash received</b>		<b>78 179</b>	<b>70 473</b>	<b>87 337</b>
<b>Cash used</b>				
Principal repayments of lease liabilities		31 829	-	-
<b>Total cash used</b>		<b>31 829</b>	<b>-</b>	<b>-</b>
<b>NET CASH FROM/(USED BY) FINANCING ACTIVITIES</b>		<b>46 350</b>	<b>70 473</b>	<b>87 337</b>
<b>Net increase (decrease) in cash held</b>		<b>(7257)</b>	<b>2280</b>	<b>(35)</b>
Cash and cash equivalents at the beginning of the reporting period		23 517	22 469	23 552
<b>CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD</b>	2.1.A	<b>16 260</b>	<b>24 749</b>	<b>23 517</b>

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

# NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

## Overview

### The basis of preparation

The financial statements are general purpose and required by section 42 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The financial statements have been prepared in accordance with:

- *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*; and
- 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. ASIO has applied the exemption available under section 105D of the PGPA Act. The effect is immaterial to the financial performance and position as disclosed in the financial statements.

### New accounting standards

#### Application of AASB 15 Revenue from Contracts with Customers

*AASB 15 Revenue from Contracts with Customers* became effective on 1 July 2019.

The application did not materially impact the financial statements of ASIO.

AASB 15 establishes a comprehensive framework for determining whether, how much and when revenue is recognised. It replaces existing revenue recognition guidance included in *AASB 118 Revenue*. The core principle of AASB 15 is that an entity recognises revenue to depict the transfer of promised goods or services to its customers in an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services.

#### Application of AASB 16 Leases

*AASB 16 Leases* became effective on 1 July 2019. It replaced *AASB 117 Leases*. AASB 16 provides a single lessee accounting model, requiring the recognition of assets and liabilities for all leases. It contains options to exclude leases where the lease term is 12 months or less, or where the underlying asset is of low value. AASB 16 substantially carries forward the lessor accounting in AASB 117, with the distinction between operating and finance leases being retained. The details of the changes in accounting policies, transitional provisions and adjustments are disclosed below and in the relevant notes to the financial statements.

ASIO adopted AASB 16 using the modified retrospective approach, under which the cumulative effect of initial application is recognised in retained earnings as at 1 July 2019. Accordingly, the comparative information presented for 2019 is not restated and is presented as previously reported under AASB 117 and related interpretations.

ASIO elected to apply the practical expedient to not reassess whether a contract is, or contains, a lease at the date of initial application. Contracts entered into before transition date that were not identified as leases under AASB 117 were not reassessed. The definition of a lease under AASB 16 was applied only to contracts entered into or changed on or after 1 July 2019.

AASB 16 provides for certain optional practical expedients, including those related to the initial adoption of the standard. ASIO utilised the following practical expedients when applying AASB 16 to leases previously classified as operating leases under AASB 117:

- applied a single discount rate to a portfolio of leases with reasonably similar characteristics;
- excluded initial direct costs from the measurement of right-of-use assets at the date of initial application for leases where a right-of-use asset was determined as if AASB 16 had been applied since the commencement date;
- relied on previous assessments on whether leases are onerous as opposed to preparing an impairment review under *AASB 136 Impairment of assets* as at the date of initial application; and
- applied the exemption not to recognise right-of-use assets and liabilities for leases with less than 12 months of lease term remaining as at the date of initial application.

On adoption of AASB 16, ASIO recognised right-of-use assets and lease liabilities in relation to leases of office space, equipment and motor vehicles, which had previously been classified as operating leases.

The lease liabilities were measured at the present value of the remaining lease payments, discounted using a zero-coupon yield rate supplied by Department of Finance. This rate was in lieu of an incremental borrowing rate which does not apply to ASIO as it does not borrow in the open market.

The right-of-use assets were measured at an amount equal to the lease liability adjusted by the amount of any lease payments before commencement date, lease incentives received and estimated restoration obligations.

The following table reconciles minimum lease commitments disclosed in ASIO's 30 June 2019 annual financial statements to the amount of lease liabilities recognised on 1 July 2019.

	1 July 2019 \$'000
Minimum operating lease commitment at 30 June 2019	523 720
Less: GST included in commitments	(46 771)
Less: commitments outside the scope of AASB 16	(106 697)
Plus: effect of extension options reasonably certain to be exercised	333 452
<b>Undiscounted lease payments</b>	<b>703 704</b>
Less: effect of discounting using the zero-coupon yield as at date of initial application	(75 717)
Plus: additional leases within scope of AASB 16	1677
<b>Lease liabilities recognised at 1 July 2019</b>	<b>629 664</b>

### Impact on transition

On transition to AASB 16 ASIO recognised right-of-use assets and additional lease liabilities. The difference was recognised in retained earnings.

	1 July 2019 \$'000
<b>Summary of impact on transition</b>	
Right-of-use assets—buildings	636 018
Right-of-use assets—property, plant and equipment	16 469
Lease liabilities	(629 664)
Retained earnings	(22 823)

### Taxation

ASIO is exempt from all forms of taxation except Fringe Benefits Tax and the Goods and Services Tax (GST).

### Events after the reporting period

There was no subsequent event that had the potential to significantly affect the ongoing structure or financial activities of ASIO.

# 1. Financial performance

	2020 \$'000	2019 \$'000
<b>1.1 EXPENSES</b>		
<b>1.1.A Employee benefits</b>		
Wages and salaries	215 450	205 231
Superannuation		
Defined contribution plans	22 709	20 631
Defined benefit plans	15 699	15 606
Leave and other entitlements	24 575	30 423
Separation and redundancies	8655	186
<b>Total employee benefits</b>	<b>287 088</b>	<b>272 077</b>
<b>1.1.B Suppliers</b>		
Goods supplied	6514	7704
Services supplied	143 387	147 421
Operating lease rentals <sup>1</sup>	1320	42 674
Workers' compensation premiums	778	847
<b>Total supplier expenses</b>	<b>151 999</b>	<b>198 646</b>
<sup>1</sup> ASIO has applied AASB 16 using the modified retrospective approach and therefore the comparative information has not been restated and continues to be reported under AASB 117.		
ASIO has no short-term lease commitments as at 30 June 2020.		
The above lease disclosures should be read in conjunction with notes 1.1.C, 1.2.B, 2.2.A and 2.4.A.		
<b>Accounting policy</b>		
ASIO has elected not to recognise right-of-use assets and lease liabilities for short-term leases that have a lease term of 12 months or less and leases of low-value (less than \$10 000). ASIO recognises the lease payments associated with these leases as an expense on a straight-line basis over the lease term.		
<b>1.1.C Finance costs</b>		
Interest on lease liabilities	8414	-
Unwinding of discount—restoration obligations	274	739
<b>Total finance costs</b>	<b>8688</b>	<b>739</b>
<b>1.1.D Write-down and impairment of other assets</b>		
Write-down and impairment of property, plant, equipment and computer software	-	539
Losses from asset sales	425	117
<b>Total write-down and impairment of other assets</b>	<b>425</b>	<b>656</b>

2020	2019
\$'000	\$'000

## 1.2 OWN-SOURCE REVENUE AND GAINS

<b>1.2.A Sale of services</b>	<b>18 019</b>	<b>15 147</b>
-------------------------------	---------------	---------------

### Accounting policy

Revenue from the sale of services is recognised by reference to the stage of completion of contracts at reporting date. This is determined by the proportion that costs incurred to date bear to the estimated total costs of the transaction.

### 1.2.B Other revenue

Subleased right-of-use assets income	4305	6015
Resources received free of charge—remuneration of auditors	135	145
Resources received free of charge—equipment	473	-
Royalties	1	1
Other	1227	1139
<b>Total other revenue</b>	<b>6141</b>	<b>7300</b>

### Subleased right-of-use assets income commitments

As lessor, subleased right-of-use assets income commitments are for office accommodation.

#### Commitments are receivable:

Within 1 year	3929	3797
Between 1 to 5 years	17 210	16 607
More than 5 years	11 074	15 606
<b>Total subleased right-of-use assets income commitments</b>	<b>32 213</b>	<b>36 010</b>

### Accounting policy

Resources received free of charge are recognised as revenue 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.

## 2. Financial position

	2020	2019
	\$'000	\$'000

### 2.1 FINANCIAL ASSETS

<b>2.1.A Cash and cash equivalents</b>	<b>16 260</b>	<b>23 517</b>
--	---------------	---------------

#### Accounting policy

Cash is recognised at its nominal amount. Cash and cash equivalents 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.

### 2.1.B Trade and other receivables

Goods and services	3639	4543
Appropriation receivable	102 018	77 623
GST receivable	4372	3728
<b>Total trade and other receivables</b>	<b>110 029</b>	<b>85 894</b>

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

Credit terms for goods and services were within 30 days (2019: 30 days).

Financial assets were assessed for impairment at 30 June 2020. No indicators of impairment have been identified.

#### Accounting policy

Trade and other receivables are:

- held for the purpose of collecting contractual cash flows where the cash flows are solely payments of principal and interest and not provided at below-market interest rates;
- adjusted on initial measurement for expected credit losses; and
- subsequently measured at amortised cost using the effective interest method adjusted for any loss allowance.

<b>2.1.C Amortisation of subleased right-of-use assets income<sup>2</sup></b>	<b>1441</b>	<b>-</b>
---	-------------	----------

<sup>2</sup> ASIO has applied AASB 16 using the modified retrospective approach and therefore the comparative information has not been restated and continues to be reported under AASB 117. The comparative amount includes amortisation of rent expense for ASIO's leases as lessee. These leases are now accounted for under AASB 16.



## 2.2 NON-FINANCIAL ASSETS

### 2.2.A Reconciliation of property, plant, equipment and computer software

	Buildings \$'000	Buildings— leasehold improvement \$'000	Property plant equipment & computer software \$'000	Total \$'000
<b>As at 1 July 2019</b>				
Gross book value	6692	160 024	371 776	538 492
Accumulated depreciation, amortisation and impairment	(437)	(20 414)	(177 581)	(198 432)
<b>Net book value 1 July 2019</b>	<b>6255</b>	<b>139 610</b>	<b>194 195</b>	<b>340 060</b>
Recognition of right-of-use assets on initial application of AASB 16	636 018	-	16 469	652 487
<b>Total 1 July 2019</b>	<b>642 273</b>	<b>139 610</b>	<b>210 664</b>	<b>992 547</b>
Additions by purchase	893	1663	66 034	68 590
Additions—internally developed	-	-	10 363	10 363
Revaluations recognised in other comprehensive income	304	14 303	5909	20 516
Depreciation and amortisation	(400)	(15 858)	(76 025)	(92 283)
Disposals—other	-	(2169)	(866)	(3035)
Right-of-use assets additions	-	-	97	97
Right-of-use assets depreciation	(44 391)	-	(2435)	(46 826)
<b>Net book value 30 June 2020</b>	<b>598 679</b>	<b>137 549</b>	<b>213 741</b>	<b>949 969</b>
Gross book value	643 149	140 715	375 026	1 158 890
Accumulated depreciation, amortisation and impairment	(44 470)	(3166)	(161 285)	(208 921)
<b>Net book value 30 June 2020</b>	<b>598 679</b>	<b>137 549</b>	<b>213 741</b>	<b>949 969</b>
<b>Carrying amount of right-of-use assets</b>	<b>591 627</b>	<b>-</b>	<b>14 131</b>	<b>605 758</b>

#### Impairment

Non-financial assets are assessed for impairment at the end of each reporting period. There are no indicators of impairment for property, plant, equipment and computer software. Any reduction in assets' carrying value due to impairment throughout the year has been accounted for in the statement of comprehensive income.

#### Sale or disposal

Property, plant, equipment and computer software of an immaterial value only is expected to be sold or disposed of within the next 12 months. No buildings are expected to be sold or disposed of within the next 12 months.

	Buildings \$'000	Buildings— leasehold improvement \$'000	Property plant equipment & computer software \$'000	Total \$'000
<b>Contractual commitments for the acquisition of property, plant, equipment and computer software</b>				
Within 1 year	-	1	5505	5506
Between 1 to 5 years	-	-	136	136
<b>Total capital commitments</b>	<b>-</b>	<b>1</b>	<b>5641</b>	<b>5642</b>

## Accounting policy

### Acquisition of assets

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.

Purchases of non-financial assets are initially recognised at cost in the statement of financial position, except for purchases costing less than \$4000, 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).

### Property, plant, equipment and computer software (excluding right-of-use assets)

Following initial recognition at cost, property, plant and equipment is carried at fair value less subsequent 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.

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

**2020**

Buildings on freehold land	<b>8–60 years</b>
Leasehold improvements	<b>lease term</b>
Plant and equipment	<b>2–25 years</b>

All assets were assessed for impairment at 30 June 2020. 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.

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

ASIO's software comprises purchased and internally developed 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 (2019: 1–10 years).

**Lease right-of-use assets**

Lease right-of-use assets are capitalised at the commencement date of the lease and comprise the initial lease liability amount, initial direct costs incurred when entering into the lease less any lease incentives received. These assets are disclosed by Commonwealth lessees as separate asset classes, and presented with corresponding assets according to the nature of the lease.

Lease right-of-use assets are measured at cost after initial recognition and depreciated on a straight-line basis over the lease term.

**Fair value measurement**

ASIO's assets are held for operational purposes and not held for the purpose of deriving a profit. The current use of all non-financial assets is considered their highest and best use.

Comprehensive valuations are carried out at least once every three years. ASIO engaged the services of Jones Lang LaSalle (JLL) to conduct a comprehensive valuation of carrying amounts for all non-financial assets (excluding software and lease right-of-use assets) as at 30 April 2020. JLL has provided written assurance to ASIO that the models developed are in compliance with *AASB 13 Fair Value Measurement*.

The methods utilised to determine and substantiate the unobservable inputs are derived and evaluated as follows:

Physical depreciation and obsolescence—Assets that do not transact with enough frequency or transparency to develop objective opinions of value from observable market evidence have been measured utilising the Current Replacement Cost approach. Under the Current Replacement Cost approach, the estimated cost to replace the asset is calculated and then adjusted to take into account physical depreciation and obsolescence. Physical depreciation and obsolescence has been determined based on professional judgement regarding physical, economic and external obsolescence factors relevant to the asset under consideration. For all leasehold improvement assets, the consumed economic benefit/asset obsolescence deduction is determined based on the term of the associated lease.

Assets classified in a particular level input in the current financial reporting period may be reclassified into a different level in subsequent periods as identified during the revaluation process.

The fair values of ASIO's assets at 30 June 2020 are detailed above in Note 2.2.A.

2020  
\$'000

2019  
\$'000

## 2.3 PAYABLES

### 2.3.A Suppliers

Trade creditors and accruals	9991	9373
------------------------------	------	------

<b>Total suppliers</b>	<b>9991</b>	<b>9373</b>
------------------------	-------------	-------------

Settlement is usually made within 30 days.

### 2.3.B Other payables

Salaries	5415	1669
Superannuation	554	275
Termination benefits	3794	185
Unearned income	435	1119
Lease incentives	-	490
Fringe benefits tax	2222	1630
Amortisation of rent expense	-	21 269

<b>Total other payables</b>	<b>12 420</b>	<b>26 637</b>
-----------------------------	---------------	---------------

## 2.4 INTEREST BEARING LIABILITIES

### 2.4.A Interest bearing liabilities

Lease liabilities—buildings	604 165	-
Lease liabilities—property, plant, equipment and computer software	14 367	-

<b>Total interest bearing liabilities</b>	<b>618 532</b>	<b>-</b>
---	----------------	----------

ASIO has applied AASB 16 using the modified retrospective approach and therefore there is no comparative information.

Total cash outflow for leases for the year ended 30 June 2020 was \$40.243 million.

## 2.5 PROVISIONS

### 2.5.A Employee provisions

Leave	95 063	91 336
Termination benefits	1482	-

<b>Total employee provisions</b>	<b>96 545</b>	<b>91 336</b>
----------------------------------	---------------	---------------

### Accounting judgements and estimates

Leave provisions involve assumptions based on the expected tenure of existing staff, patterns of leave claims and payouts, future salary movements and future discount rates.

### Accounting policy

Liabilities for 'short-term employee benefits' (as defined in *AASB 119 Employee Benefits*) and termination benefits expected within 12 months of the end of the reporting period are measured at nominal amounts.

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 will 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 leave has been determined by reference to the work of an actuary as at May 2020. The estimate of present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

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 in the Department of Finance's administered schedules and notes.

ASIO makes employer contributions to employees' superannuation schemes 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.

	2020 \$'000	2019 \$'000
<b>2.5.B Restoration obligations</b>	<b>7225</b>	<b>6794</b>
Carrying amount 1 July	6794	6072
Additional provisions made	157	-
Reduction in value	-	(17)
Unwinding of discount or change in discount rate	274	739
<b>Closing balance</b>	<b>7225</b>	<b>6794</b>

ASIO has a number of agreements for the leasing of premises which contain provisions requiring restoration of the premises to original condition at the conclusion of the lease. ASIO has made a provision to reflect the present value of this obligation.

## 3. Funding

### 3.1 APPROPRIATIONS

#### 3.1.A Annual departmental appropriations

	Ordinary annual services \$'000	Capital budget <sup>3</sup> \$'000	Equity injections \$'000
<b>2020</b>			
<b>Appropriation Act</b>			
Annual appropriation <sup>4</sup>	473 011	61 329	10 870
<b>PGPA Act</b>			
Section 74 transfers	31 331	-	-
<b>Total appropriation</b>	<b>504 342</b>	<b>61 329</b>	<b>10 870</b>
Appropriation applied (current and prior years)	(472 670)	(69 829)	(8350)
<b>Variance</b>	<b>31 672</b>	<b>(8500)</b>	<b>2520</b>

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

<sup>4</sup> \$6.141 million was returned to Government in accordance with PGPA Act section 51.

Operating appropriation remains unspent in 2020 due to reduced supplier purchases resulting from COVID-19 restrictions.

Variances in 2020 Capital appropriations are due to prior year appropriations applied in the current year.

The Department of Foreign Affairs and Trade spends money from the Consolidated Revenue Fund on behalf of ASIO in relation to services overseas: \$7.583 million (2019: \$8.014 million).

#### 2019

##### Appropriation Act

Annual appropriation	435 196	85 572	5367
----------------------	---------	--------	------

##### PGPA Act

Section 74 transfers	43 188	-	-
----------------------	--------	---	---

<b>Total appropriation</b>	<b>478 384</b>	<b>85 572</b>	<b>5367</b>
Appropriation applied (current and prior years)	(450 183)	(80 572)	(6765)
<b>Variance</b>	<b>28 201</b>	<b>5000</b>	<b>(1398)</b>

The 2019 operating appropriation was unspent in 2019 due to the timing of supplier purchases. Capital appropriations were unspent due to the timing of asset purchases.

	2020 \$'000	2019 \$'000
<b>3.1.B Unspent departmental annual appropriations (recoverable GST exclusive)</b>		
Appropriation Act (No. 1) 2018–19	-	96 140
Appropriation Act (No. 2) 2018–19	-	5 000
Appropriation Act (No. 1) 2019–20	92 888	-
Appropriation Act (No. 2) 2019–20	5 481	-
Appropriation Act (No. 3) 2019–20	17 870	-
Appropriation Act (No. 4) 2019–20	2 039	-
<b>Total</b>	<b>118 278</b>	<b>101 140</b>

### 3.1.C Net cash appropriation arrangements

#### **Total surplus (deficit) excluding depreciation, amortisation and lease principal repayments**

	<b>17 106</b>	<b>(14 449)</b>
Depreciation and amortisation (excluding right-of-use leased assets)	(92 283)	(104 066)
Depreciation—right-of-use leased assets	(46 826)	-
Principal repayments—leases	31 926	-
Deficit as per statement of comprehensive income	(90 077)	(118 515)

From 2010–11, the Government introduced net cash appropriation arrangements where revenue appropriations for depreciation/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.

The inclusion of depreciation/amortisation expenses related to right-of-use leased assets and the lease liability principal repayment amount reflects the cash impact on implementation of *AASB 16 Leases*. It does not directly reflect a change in appropriation arrangements.

## 4. Managing uncertainties

2020  
\$'000

2019  
\$'000

### 4.1 CONTINGENT ASSETS AND LIABILITIES

#### Quantifiable contingencies

ASIO's contingent liabilities relate to claims for damages or costs. The amount represents an estimate of ASIO's liability based on precedent in such cases. ASIO is defending the claims.

#### Contingent liabilities

Balance from previous period	-	60
New contingent liabilities recognised	200	-
Liabilities realised	-	(60)
<b>Total contingent liabilities</b>	<b>200</b>	<b>-</b>

#### Unquantifiable contingencies

At 30 June 2020, ASIO had a number of legal claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate the amounts of any eventual payments that may be required in relation to these claims.

#### Accounting policy

Contingent liabilities and contingent assets are not recognised in the statement of financial position 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.

### 4.2 FINANCIAL INSTRUMENTS

#### 4.2.A Categories of financial instruments

##### Financial assets at amortised cost

Cash	16 260	23 517
Trade receivables	3639	4543
Accrued revenue	602	575
<b>Total financial assets</b>	<b>20 501</b>	<b>28 635</b>

##### Financial liabilities at amortised cost

Trade creditors and accruals	9991	9373
<b>Total financial liabilities</b>	<b>9991</b>	<b>9373</b>

The net fair values of the financial assets and liabilities are at their carrying amounts. ASIO derived no interest income from financial assets in either the current or prior year.

There was no net gain or loss from financial assets or liabilities through profit or loss for the period ending 30 June 2020 (2019 :Nil).



**Accounting policy****Financial assets**

ASIO classifies its financial assets as 'measured at amortised cost'. Financial assets included in this category must meet two criteria:

- the financial asset is held in order to collect the contractual cash flows; and
- the cash flows are solely payments of principal and interest on the principal outstanding amount.

Amortised cost is determined using the effective interest method with income recognised on an effective interest rate basis.

Financial assets are recognised when ASIO becomes party to a contract and, as a consequence, has a legal right to receive or obligation to pay cash and derecognised when the contractual rights to the cash flows from the financial asset expire or are transferred upon trade date.

Financial assets are assessed for impairment at the end of each reporting period. Allowances are made when collectability of the debt is no longer probable.

Financial assets are assessed for impairment at the end of each reporting period based on an amount equal to the lifetime expected credit losses. A write-off directly reduces the gross carrying amount of the financial asset.

**Financial liabilities**

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). Supplier and other payables are derecognised on payment.

## 5. Other information

2020  
\$'000

2019  
\$'000

### 5.1 KEY MANAGEMENT PERSONNEL REMUNERATION

Key management personnel are those persons having authority and responsibility for planning, directing and controlling the activities of ASIO, directly or indirectly. ASIO has determined key management personnel to be the Director-General and members of the Executive Committee.

Short-term employee benefits	2183	1975
Long-term employee benefits	68	265
Termination benefits	301	-
Post-employment benefits	339	334
<b>Total key management personnel remuneration expenses<sup>5</sup></b>	<b>2891</b>	<b>2574</b>

The number of key management positions as at 30 June is 6 (2019: 5).

Membership of the Executive Committee changed throughout 2019–20. Several key management positions were occupied by different officers for portions of the year.

<sup>5</sup> The above key management personnel remuneration excludes the remuneration and other benefits of the:

- portfolio ministers whose remuneration and other benefits are set by the Remuneration Tribunal and are not paid by ASIO; and
- external member of ASIO's Executive Committee (1 Jul 19 – 28 May 20), who is an executive of another Australian Government entity. No remuneration or other benefits were paid by ASIO.

### 5.2 RELATED PARTY DISCLOSURES

#### Related party relationships

ASIO is an Australian Government-controlled entity. ASIO's related parties are key management personnel including the portfolio ministers and Executive Committee, and other Australian Government entities.

#### Transactions with key management personnel

Given the breadth of government activities, key management personnel and their associates may transact with the government sector in the same capacity as ordinary citizens. Such transactions include the payment or refund of taxes, receipt of a Medicare rebate or higher education loans. These transactions are not disclosed in this note.

All related party transactions with key management personnel during 2019–20 were in the ordinary course of business and do not require separate disclosure.

### Transactions with other Australian Government entities

ASIO transacts with Commonwealth Government entities at arm's length for the provision of goods and services in the normal course of business. These transactions are not disclosed in this note.

ASIO has a significant relationship with the Department of Finance as lessor of the organisation's headquarters in Canberra. Lease expenses were \$23.430 million in 2019–20.

### 5.3 MAJOR BUDGET VARIANCES

The following provides an explanation of variances between the original budget as presented in the 2019–20 Portfolio Budget Statements (PBS) and the 2019–20 final actual result. The budget is not audited. Explanations are provided for major budget variances only. Variances are treated as major when it is considered important for the reader's understanding or is relevant to an assessment of the discharge of accountability and to an analysis of ASIO's performance.

The nature and timing of the Commonwealth's budget process can also contribute to the variances. ASIO's major budget impacts include:

- estimated actual outcomes were published in the 2019–20 PBS before the closing 2018–19 and opening 2019–20 statement of financial position was known. Therefore, the opening balances of the statement of financial position were estimates.
- the original budget as presented in the 2019–20 PBS is amended by Government throughout the year. ASIO's budget for 2019–20 was updated as part of the 2019–20 Mid-Year Economic Fiscal Outlook (MYEFO).

Other considerable events during 2019–20 not factored into the budget figures which have significantly impacted the 2019–20 results are:

- implementation on 1 July 2019 of the new accounting standard *AASB 16 Leases* which changed the financial accounting for leases. The standard requires the recognition of right-of-use assets and lease liabilities in relation to leases of office space, equipment and motor vehicles, which had previously been classified as operating leases. The adoption of AASB 16 impacted non-financial assets, liabilities, supplier expenditure and depreciation. Refer Overview for further details of accounting treatment. Required adjustments were unknown during development of the original budget; and
- the spread of the novel coronavirus disease (COVID-19) has caused major disruption to economic activity. The considerable uncertainty and travel restrictions have contributed to underspends in some expense categories that could not have been predicted during development of the 2019–20 budget.

## Expenses

The total variance between actual expenses and the original budget is an increase of \$7.927 million (1%), but comprises variances between expense categories:

- employee benefits were \$11.246 million higher than original budget due to redundancy payments made or provided for at balance date;
- supplier expenses were \$59.610 million lower than original budget mainly as a result of the adoption of AASB 16 (\$40.243 million). Additionally, other expense items were lower than budget as a result of COVID-19 restrictions; and
- depreciation and amortisation expenses were \$47.179 million higher than original budget primarily due to the recognition of right-of-use assets and associated depreciation in compliance with AASB 16 (\$46.826 million).

## Income

Income is \$9.781 million (2%) higher than original budget. The increase is due to:

- an increase of \$9.376 million in appropriation funding as a result of new Government decisions;
- an increase in other revenue of \$4.369 million relating to rental income which was unknown at the time of budget preparation; and
- revenue from the sale of services was \$3.880 million less than budget. This budget is dependent on requests and activities undertaken by external parties which was less than anticipated, in part as a result of COVID-19 restrictions.

## Assets

Total assets are \$650.366 million higher (141%) than original budget. Financial assets are \$38.538 million higher than budget, in part due to the difference between the actual and budgeted opening balances. The largest variance is within appropriation receivable which includes undrawn appropriation as a result of reduced expenditure relating to COVID-19 restrictions. These funds form part of the receivables balance and will be available in 2020–21.

Non-financial assets are \$611.828 million higher than original budget mainly as a result of the implementation of AASB 16 and the capitalisation of right-of-use assets for office space, equipment and motor vehicles (\$605.757 million).

## Liabilities

Total liabilities are \$631.025 million higher (554%) than original budget. The increase is attributed to:

- the recognition of lease liabilities on implementation of AASB 16 (\$618.532 million); and
- an increase of \$14.824 million in employee provisions primarily due to the decrease in the Government bond rate which is a component of the discount rate used to estimate the provision's net present value. A reduction in uptake of leave during the COVID-19 restrictions also contributed to the higher than expected final actual balance.

**Statement of changes in equity**

Total equity is over budget by \$19.341 million. The increase primarily relates to the revaluation of non-financial assets which resulted in a \$20.516 million increase to the fair value of non-financial assets. The remaining increase relates to equity injections as a result of new Government decisions.

**Statement of cash flows**

The amounts reported in the statement of cash flows are interrelated with figures disclosed in the statement of comprehensive income and statement of financial position. Consequently, cash flow variances are attributable to the relevant variance explanations provided above.





A

## Appendices





# Appendix A: ASIO resource statement

	Actual available appropriation 2020 \$'000	Payments made 2020 \$'000	Balance remaining 2020 \$'000
<b>Departmental</b>			
Annual appropriations—ordinary annual services <sup>1</sup>			
Prior year appropriation	72 623	72 623	-
Departmental appropriation <sup>2</sup>	473 011	390 013	82 998
Section 74 external revenue <sup>3</sup>	22 776	22 776	-
Departmental capital budget <sup>4</sup>	61 329	49 829	11 500
Cash on hand	23 517	7257	16 260
Annual appropriations—other services—non-operating <sup>5</sup>			
Prior year appropriation	5000	5000	-
Equity injections	10 870	3350	7520
<b>Total net resourcing and payments for ASIO</b>	<b>669 126</b>	<b>550 848</b>	<b>118 278</b>

<sup>1</sup> Supply Act (No.1), Appropriation Act (No.1) and Appropriation Act (No.3)

<sup>2</sup> Excludes departmental capital budget (DCB)

<sup>3</sup> External receipts under section 74 of the *Public Governance, Performance and Accountability Act 2013*

<sup>4</sup> Departmental capital budgets are not separately identified in Supply Act (No.1), Appropriation Act (No.1) and Appropriation Act (No.3) and form part of ordinary annual services items. For accounting purposes, this amount has been designated as a 'contribution by owner'.

<sup>5</sup> Supply Act (No.2), Appropriation Act (No.2) & Appropriation Act (No.4)

# Appendix B: expenses by outcomes

Outcome 1: To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to Government	Budget* 2020 \$'000	Actual expenses 2020 \$'000	Variation 2020 \$'000
<b>Program 1.1: Security Intelligence</b>			
Departmental expenses			
Departmental appropriation	485 242	424 815	60 427
Section 74 external revenue <sup>1</sup>	23 671	22 776	895
Expenses not requiring appropriation in the budget year <sup>2</sup>	92 076	139 718	(47 642)
<b>Total for Program 1.1</b>	<b>600 989</b>	<b>587 309</b>	<b>13 680</b>
<b>Total expenses for Outcome 1</b>	<b>600 989</b>	<b>587 309</b>	<b>13 680</b>

\* Full-year budget, including any subsequent adjustments made at Additional Estimates and reductions under *Public Governance, Performance and Accountability Act 2013* section 51

<sup>1</sup> Expenses incurred in relation to receipts retained under *Public Governance, Performance and Accountability Act 2013* section 74

<sup>2</sup> Expenses not requiring appropriation in the budget year are depreciation, amortisation expenses and resources received free of charge.

## Appendix C: executive remuneration

### Key management personnel remuneration

Categories of ASIO key management personnel include:

- the Director-General of Security;
- members of the Executive Committee;
- Senior Executive Service (SES) employees; and
- other highly paid staff.

### Remuneration policies, practices and governance

The Director-General's remuneration is set by the Remuneration Tribunal under section 13 of the *Remuneration Tribunal Act 1973*.

Remuneration of ASIO's senior executive employees is established through determinations made under section 84 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), and guided by the Australian Government's Workplace Bargaining Policy 2018.

There were no general increases to SES remuneration during the 2019–20 reporting period.

The following tables show the remuneration for key management personnel, senior executives and other highly paid staff in 2019–20 in accordance with the Public Governance, Performance and Accountability Rule (PGPA) Rule.

## Information about remuneration for key management personnel<sup>1</sup>

Name	Position title	Short-term benefits			Post-employment benefits			Termination benefits		Total remuneration
		Base salary <sup>2</sup>	Bonuses	Other benefits and allowances	Superannuation contributions	Other long-term service leave <sup>3</sup>	Other long-term benefits	benefits	benefits	
		\$	\$	\$	\$	\$	\$	\$	\$	\$
Mike BURGESS	Director-General <sup>4</sup>	496 510	0	0	73 309	16 118	0	0	0	585 937
Duncan LEWIS	Director-General <sup>4</sup>	136 289	0	0	18 091	2965	0	0	0	157 346
Heather COOK	Deputy Director-General	379 246	0	3867	67 135	23 750	0	0	0	473 999
Wendy SOUTHERN	Deputy Director-General	281 518	0	3702	46 301	6531	0	0	0	338 052
Peter VICKERY	Deputy Director-General	336 903	0	34 140	64 497	7984	0	301 229	0	744 753
Hazel BENNETT	Deputy Director-General	56 265	0	0	10 129	899	0	0	0	67 293
Name withheld <sup>5</sup>	Strategic Advisor	103 387	0	876	15 627	2965	0	0	0	122 854
Name withheld <sup>6</sup>	Chief Transformation Officer	299 157	0	3867	35 502	6529	0	0	0	345 055
Name withheld <sup>7</sup>	First Assistant Director-General Strategy & Engagement	47 160	0	0	7936	757	0	0	0	55 854

<sup>1</sup> This table reflects the transition of Directors-General, and changes to associated governance arrangements during the reporting period (see p. 57).

<sup>2</sup> This includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*.

<sup>3</sup> This does not represent one year's leave accrual at officer's current salary. The value is in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*. Discount rate variations throughout the year will affect the value.

<sup>4</sup> The pro rata remuneration in this table differs from that shown in Remuneration Tribunal (Remuneration and Allowances for Holders of Full-time Public Office) Determination 2019 because the Department of Finance (in *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*) specifies a different basis for determining the value of annual and long service leave, and superannuation.

<sup>5</sup> The Strategic Advisor is a non-declared officer. To comply with section 92 of the *ASIO Act 1979* and the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the CTO's name has not been provided in the annual report.

<sup>6</sup> The ASIO Chief Transformation Officer (CTO) is a non-declared officer. To comply with section 92 of the *ASIO Act 1979* and the determination issued to ASIO under section 105D for the *Public Governance Performance and Accountability Act 2013*, the CTO's name has not been provided in the annual report.

<sup>7</sup> The First Assistant-Director General Strategy and Engagement is a non-declared officer. To comply with section 92 of the *ASIO Act 1979* and the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the name of the First Assistant-Director General Strategy and Engagement has not been provided in the annual report.

## Information about remuneration for senior executives

Remuneration band	Number of senior executives	Short-term benefits			Post-employment benefits		Other long-term benefits		Termination benefits		Total remuneration
		Average base salary <sup>1</sup>	Average bonuses	Average other benefits and allowances	Average superannuation contributions	Average	Average long service leave <sup>2</sup>	Average other long-term benefits	Average termination benefits	Average	
		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
\$0 to \$225 000	16	43 677	0	1753	7375	2315	0	0	0	0	55 119
\$225 001 to \$250 000	5	196 202	0	3631	36 327	4119	0	0	0	0	240 279
\$250 001 to \$275 000	10	213 255	0	2987	36 261	9957	0	0	0	0	262 460
\$275 001 to \$300 000	19	218 668	0	14 857	39 766	16 827	0	0	0	0	290 118
\$300 001 to \$325 000	7	238 481	0	7590	42 007	20 971	0	0	0	0	309 049
\$325 001 to \$350 000	3	260 242	0	6678	40 358	25 349	0	0	0	0	332 626
\$350 001 to \$375 000	3	264 899	0	11 932	43 590	40 072	0	0	0	0	360 493
\$375 001 to \$400 000	4	287 003	0	17 487	43 011	27 548	0	0	14 038	0	389 088
\$425 001 to \$450 000	3	194 889	0	16 802	40 820	7302	0	0	177 762	0	437 575
\$450 001 to \$475 000	4	292 927	0	19 225	45 229	13 076	0	0	91 659	0	462 117
\$475 001 to \$500 000	4	291 484	0	49 589	45 137	10 701	0	0	93 649	0	490 560
\$500 001 to \$525 000	2	253 853	0	10 667	48 221	10 079	0	0	181 774	0	504 594
\$525 001 to \$550 000	2	258 346	0	3867	46 784	7449	0	0	219 236	0	535 682
\$575 001 to \$600 000	3	275 578	0	11 638	52 991	14 638	0	0	234 372	0	589 218
\$600 001 to \$625 000	1	258 279	0	29 125	52 991	14 728	0	0	248 044	0	603 167

<sup>1</sup> This includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*.

<sup>2</sup> This does not represent one year's leave accrual at officer's current salary. The value is in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*. Discount rate variations throughout the year will affect the value.

### Information about remuneration for other highly paid staff

Remuneration band	Number of highly paid staff	Short-term benefits			Post-employment benefits			Other long-term benefits			Termination benefits		Total remuneration
		Average base salary <sup>1</sup>	Average bonuses	Average other benefits and allowances	Average superannuation contributions	Average long service leave <sup>2</sup>	Average other long-term benefits	Average termination benefits	Average total remuneration				
		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
\$225 001 to \$250 000	15	187 544	0	8 537	32 487	9 943	0	0	238 512				
\$250 001 to \$275 000	7	209 836	0	16 320	26 364	7 645	0	0	260 164				
\$275 001 to \$300 000	6	219 903	0	9 855	24 702	7 129	0	21 788	283 377				
\$300 001 to \$325 000	5	221 086	0	24 170	26 890	7 253	0	31 306	310 705				
\$325 001 to \$350 000	3	153 339	0	0	23 464	3 782	0	157 510	338 095				
\$350 001 to \$375 000	4	184 599	0	779	25 149	3 853	0	149 272	363 652				
\$375 001 to \$400 000	3	198 363	0	21 011	27 659	5 267	0	142 131	394 431				
\$400 001 to \$425 000	3	217 670	0	13 840	29 001	5 242	0	150 677	416 432				
\$425 001 to \$450 000	3	161 844	0	7 286	30 960	3 906	0	230 625	434 620				
\$450 001 to \$475 000	1	170 306	0	3 867	33 224	4 636	0	255 289	467 322				

<sup>1</sup> This includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*.

<sup>2</sup> This does not represent one year's leave accrual at officer's current salary. The value is in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*. Discount rate variations throughout the year will affect the value.

# Appendix D: ASIO's salary classification structure

## ASIO's salary classifications

Senior Executive Service	Minimum salary	Maximum salary <sup>1</sup>
SES Band 3	\$327 377	\$393 240
SES Band 2	\$254 717	\$279 500
SES Band 1	\$203 774	\$227 697
<b>Senior employees</b>		
AEE3		\$156 789
AEE2	\$132 494	\$156 789
AEE1	\$115 595	\$129 172
<b>Employees</b>		
AE6	\$90 945	\$102 480
AE5	\$82 281	\$88 333
AE4	\$74 981	\$80 464
AE3	\$66 317	\$72 466
AE2	\$58 330	\$64 597
AE1	\$50 342	\$55 911
<b>Intelligence employees</b>		
IE	\$90 945	\$102 480
IE trainees	\$82 281	\$96 879
<b>Information technology employees</b>		
SITEA		\$156 789
SITEB	\$132 494	\$156 789
SITEC	\$115 595	\$129 172
ITE2	\$90 945	\$102 480
ITE1	\$79 206	\$87 086
<b>Engineers</b>		
SIE(E)5		\$156 789
SIE(E)4	\$132 494	\$156 789
SIE(E)3	\$115 595	\$129 172
SIE(E)2	\$90 945	\$102 480
SIE(E)1	\$79 206	\$87 086
<b>Salary range</b>		
Minimum/maximum range	\$50 342	\$393 240

Note: Figures are at 30 June 2020. The salary figures include a 7.5 per cent service allowance. The service allowance is paid to all employees and recognises the imposition of security, professional and personal restrictions applicable to working in ASIO.

<sup>1</sup> This is the maximum salary (plus service allowance) that anyone in a classification can receive. It applies to employees with the Organisation on and before 30 June 2020, and includes base salary and service allowance per annum.

# Appendix E: workforce statistics by headcount

## PGPA Rule section 17AG(4)(b)(i)–(iv)

### Classification and gender of ongoing employees— current reporting period (2019–20)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
SES 3	1	0	1	2	0	2	0	0	0	3
SES 2	10	0	10	5	0	5	0	0	0	15
SES 1	24	0	24	20	0	20	0	0	0	44
AEE1–3	367	23	390	200	76	266	0	0	0	656
AE1–6	590	20	610	487	165	652	0	0	0	1262
<b>Total</b>	<b>992</b>	<b>43</b>	<b>1035</b>	<b>704</b>	<b>241</b>	<b>945</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1980</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

## PGPA Rule section 17AG(4)(b)(i)–(iv)

### Classification and gender of non-ongoing employees— current reporting period (2019–20)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
SES 3	0	0	0	0	0	0	0	0	0	0
SES 2	0	0	0	0	0	0	0	0	0	0
SES 1	0	0	0	0	0	0	0	0	0	0
AEE1–3	2	5	7	0	1	1	0	0	0	8
AE1–6	5	6	11	1	4	5	0	0	0	16
<b>Total</b>	<b>7</b>	<b>11</b>	<b>18</b>	<b>1</b>	<b>5</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>24</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.



## PGPA Rule section 17AG(4)(b)(i)–(iv)

### Classification and gender of ongoing employees— previous reporting period (2018–19)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
SES 3	3	0	3	1	0	1	0	0	0	4
SES 2	8	0	8	5	0	5	0	0	0	13
SES 1	25	0	25	20	1	21	0	0	0	46
AEE1–3	389	18	407	183	78	261	0	0	0	639
AE1–6	575	24	599	471	159	630	0	0	0	1229
<b>Total</b>	<b>1000</b>	<b>42</b>	<b>1042</b>	<b>680</b>	<b>238</b>	<b>918</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1960</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

## PGPA Rule section 17AG(4)(b)(i)–(iv)

### Classification and gender of non-ongoing employees— previous reporting period (2018–19)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
SES 3	0	0	0	0	0	0	0	0	0	0
SES 2	0	0	0	0	0	0	0	0	0	0
SES 1	1	0	1	0	0	0	0	0	0	1
AEE1–3	2	5	7	0	1	1	0	0	0	8
AE1–6	5	6	11	1	4	5	0	0	0	16
<b>Total</b>	<b>8</b>	<b>11</b>	<b>19</b>	<b>1</b>	<b>5</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>25</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

## PGPA Rule section 17AG(4)(b)(ii)–(v)

### All ongoing employees—current reporting period (2019–20)

	Male			Female			Indeterminate			
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	Total
ACT	681	32	713	542	183	725	0	0	0	1438
Other	311	11	322	162	58	220	0	0	0	542
<b>Total</b>	<b>992</b>	<b>43</b>	<b>1035</b>	<b>704</b>	<b>241</b>	<b>945</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1980</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the location of ASIO employees outside the Australian Capital Territory including overseas is classified and has been reported collectively in the 'Other' category.

## PGPA Rule section 17AG(4)(b)(ii)–(v)

### All non-ongoing employees—current reporting period (2019–20)

	Male			Female			Indeterminate			
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	Total
ACT	2	9	11	0	5	5	0	0	0	16
Other	5	2	7	1	0	1	0	0	0	8
<b>Total</b>	<b>7</b>	<b>11</b>	<b>18</b>	<b>1</b>	<b>5</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>24</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the location of ASIO employees outside the Australian Capital Territory including overseas is classified and has been reported collectively in the 'Other' category.

## PGPA Rule section 17AG(4)(b)(ii)–(v)

### All ongoing employees—previous reporting period (2018–19)

	Male			Female			Indeterminate			
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	Total
ACT	687	28	715	518	179	697	0	0	0	1412
Other	313	14	327	162	59	221	0	0	0	548
<b>Total</b>	<b>1000</b>	<b>42</b>	<b>1042</b>	<b>680</b>	<b>238</b>	<b>918</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1960</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the location of ASIO employees outside the Australian Capital Territory including overseas is classified and has been reported collectively in the 'Other' category.

## PGPA Rule section 17AG(4)(b)(ii)–(v)

### All non-ongoing employees—previous reporting period (2018–19)

	Male			Female			Indeterminate			
	Full-time	Part-time	<b>Total male</b>	Full-time	Part-time	<b>Total female</b>	Full-time	Part-time	<b>Total indeterminate</b>	<b>Total</b>
ACT	3	9	<b>12</b>	1	5	<b>6</b>	0	0	<b>0</b>	<b>18</b>
Other	5	2	<b>7</b>	0	0	<b>0</b>	0	0	<b>0</b>	<b>7</b>
<b>Total</b>	<b>8</b>	<b>11</b>	<b>19</b>	<b>1</b>	<b>5</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>25</b>

Note: To avoid prejudice to ASIO's activities and comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the location of ASIO employees outside the Australian Capital Territory including overseas is classified and has been reported collectively in the 'Other' category.

## PGPA Rule section 17AG(4)(b)(vi)

### Indigenous employment—current reporting period (2019–20)

	<b>Total</b>
Ongoing	<b>9</b>
Non-ongoing	<b>0</b>
<b>Total</b>	<b>9</b>

## PGPA Rule section 17AG(4)(b)(vi)

### Indigenous employment—previous reporting period (2018–19)

	<b>Total</b>
Ongoing	<b>7</b>
Non-ongoing	<b>0</b>
<b>Total</b>	<b>7</b>

## Appendix F: work health and safety

ASIO's workplace safety culture is key to ensuring the health and safety of ASIO's most important asset, its people.

ASIO operates in a range of work environments, and work health and safety considerations are integrated into the planning and delivery of ASIO's activities. Our safety risk management strategies reinforce legislative compliance and a culture of continual improvement. Our focus is on identifying and monitoring key risk factors, implementing mitigation strategies, and promoting safe behaviour by our workforce.

### Health and wellbeing program

We are committed to encouraging positive physical and psychological health outcomes across our workforce. The corporate health and wellbeing program assists through education and participation. It encourages staff to:

- be motivated to make positive health, lifestyle and fitness decisions;
- develop an awareness of relevant health and wellbeing issues, including psychological resilience;
- develop their knowledge of workplace safety through training;
- engage with available support services, including ASIO's Employee Assistance Program and Manager Assist service; and
- participate in the in-house influenza vaccination program.

### Safety risk management

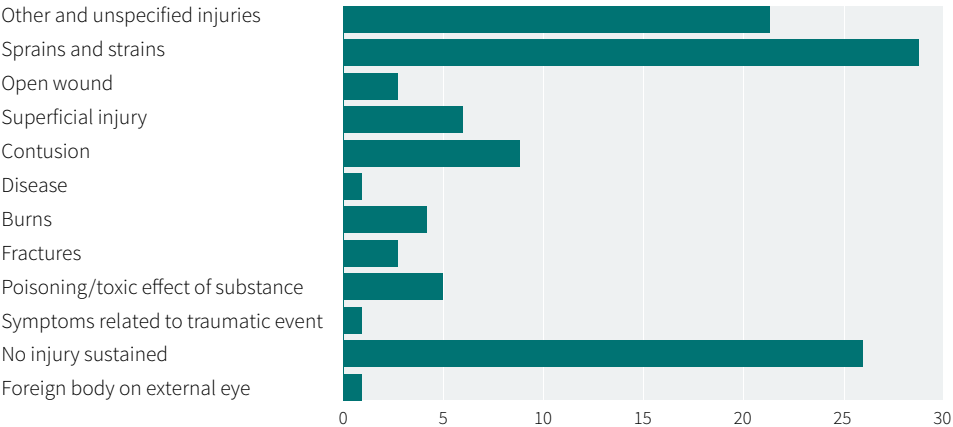
During 2019–20, ASIO responded to a range of health and safety challenges—in particular, the threat of bushfires, poor outdoor air quality due to smoke, and the ongoing complexities of the COVID-19 pandemic. In each case, the Organisation was proactive in considering safety risks and engaged the workforce to make appropriate and effective decisions.

Building on a suite of existing programs, ASIO is developing and implementing prevention initiatives which will reinforce psychological resilience in the workforce.

### Incidents

In accordance with legislated notification obligations, ASIO reported three incidents to Comcare in 2019–20. No incident investigations were undertaken by Comcare, and no notices were issued to ASIO under the *Work Health and Safety Act 2011*.

Table 5: Total number of injuries by type



## Ethics and conduct

ASIO expects the highest standards of behaviour, and actively responds to allegations of bullying, harassment and other forms of inappropriate behaviour. ASIO’s expectations are set out in policies on ethics and conduct as well as in ASIO’s defined Values, Code of Conduct and Leadership Charter.

ASIO uses several systems and processes for identifying, managing and responding to allegations of inappropriate behaviour and misconduct, including early intervention, dispute resolution, coaching and conflict management, and management of complaints and misconduct investigations.

In 2019–20, all employees undertook mandatory training clarifying employee conduct expectations. This training included:

- ASIO’s Values and Code of Conduct requirements;
- mechanisms available to make a public interest disclosure;

- managing workplace discrimination, harassment and bullying; and
- work health and safety obligations.

In addition, training was provided on conduct and behaviour through ASIO’s induction and management training programs.

## Harassment and Discrimination Advisor Network

ASIO’s network of Harassment and Discrimination Advisors (HaDA) is an Organisational resource designed to provide employees with information and impartial support in relation to discrimination, harassment, bullying and other forms of inappropriate behaviour. The HaDAs also provide referral advice and clarification of policies and complaint procedures.

## Appendix G: recruitment, advertising and market research

Over the reporting year, ASIO successfully refined and tailored recruitment campaigns and implemented strategies to attract and select new staff, particularly through leadership and specialist technical campaigns. In the financial year 2019–20, ASIO expended \$313 025 on marketing and advertising for recruitment activities and campaigns.

Further information on these advertising campaigns is available at [www.asio.gov.au](http://www.asio.gov.au) and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance’s website.

ASIO enhanced its outreach to universities, with a particular focus on science, technology, engineering and maths (STEM)–related fields. ASIO also extended its outreach on STEM fields to high schools through an information evening on career paths in ASIO and the broader intelligence community.

An innovative recruitment campaign during 2019–20 focused on ASIO’s technical workforce, providing a pipeline of potential technical talent for the Organisation. The approach incorporated digital recruiting to cater to an increasingly neurodiverse technical community.

- Prompted by COVID-19 restrictions, ASIO developed a fully virtual assessment centre process to recruit Technical Graduates commencing in 2021. As well as addressing physical distancing restrictions, the virtual process developed by ASIO recognised and applied improved technical standards and user interface to better assess and shortlist candidates in a remote setting.

Non-intelligence roles remain an integral part of ASIO’s recruitment focus, in order to support our intelligence functions.

In 2019–20, ASIO expanded its graduate programs and introduced a corporate stream to provide a career pathway to functions such as finance, human resources, procurement and legal.

## Appendix H: ecologically sustainable development and environmental performance

ASIO is committed to moving towards the goal of being more environmentally sustainable. We strive to operate in an environmentally responsible manner, making every effort to use our resources more efficiently and manage our waste effectively.

Theme	Performance measure	Indicator(s)	2018–19	2019–20
<b>Energy efficiency</b>	Total consumption of building energy	Amount of electricity consumed (kWh)	24 888 810	24 779 371
		Amount of gas consumed (MJ)	10 847 748	13 094 381
		Amount of other fuels (diesel) consumed (L)	13 579	89 518
	Total production/consumption of green energy	Amount of green energy produced and consumed (kWh) during the reporting period from solar panels and cogeneration plant	255 853	377 471
	Greenhouse gas emissions	Amount of greenhouse gases produced (tonnes)	27 332.9	26 417.3
	Environmental performance targets—tenant light & power (TL&P) and central services	TL&P less than 7500 MJ/person/annum	11 740	12 046
		Central services less than 400 MJ/m <sup>2</sup> /annum	529	498
	<b>Energy rating</b>	NABERS <sup>1</sup> energy for offices (1–6)	3.5 stars	3.5 stars

<sup>1</sup> The National Australian Built Environment Rating System (NABERS) measures a building's energy efficiency, carbon emissions, water consumption, and waste produced and delivers a performance based on a rating from 1 to 6, expressed as a number of stars for comparison with similar buildings.

Theme	Performance measure	Indicator(s)	2018–19	2019–20
	<b>Steps taken to reduce effect</b>	<b>Measures to review and improve reducing the effect</b>		
	ASIO employees are required to undertake mandatory Environmental Management eLearning.	Increased use of video web-conferencing systems to offset carbon emission previously generated by inter-office travel  Participation in national environmental events such as Earth Hour, which is encouraged		
<b>Waste</b>	Total waste production—this includes all waste (i.e. unwanted by-products) produced when undertaking the functions of the agency	Amount of waste produced (tonnes)	103.9	197.3
	Un-recyclable waste production—this includes all wastes that are not re-used or recycled	Amount of waste going to landfill (tonnes)	83.2	77.1
	Recyclable waste production (excluding office paper)	Amount of waste going to recycling facilities (tonnes)	20.7	120.2
	Paper usage	Amount of waste paper going to recycling facilities (tonnes)	20.9	10.9
		Amount of paper sourced from recyclable sources (tonnes)	4.2	2.2
		Percentage of paper sourced from recyclable sources	20%	20%
	Relative waste production	Amount of the total waste (kg) per employee	62.2	89.5
	<b>Waste rating</b>	NABERS waste rating (1–6)	1 star	3 stars



Theme	Performance measure	Indicator(s)	2018–19	2019–20
	<b>Steps taken to reduce effect</b> <p>Implemented ‘follow-me’ printing and double-sided printing and copying as the default setting on printers to reduce waste and paper expenses</p> <p>Sourced office copy paper from sustainably managed sources</p> <p>Introduced polystyrene recycling and investigated options to effectively manage e-waste.</p>	<b>Measures to review and improve reducing the effect</b> <p>Developed a waste management strategy to align with NABERS waste assessment</p> <p>Built a culture of environmental awareness across our Organisation through sustainable initiatives based on the following principles:</p> <ul style="list-style-type: none"> <li>■ reduce</li> <li>■ re-use</li> <li>■ recycle</li> <li>■ recover</li> <li>■ disposal.</li> </ul>		
<b>Water</b>	Total consumption of water—this includes all water consumed when undertaking agency functions	Amount of water consumed (kL)	52 175	54 240
	Rainwater capture and use—includes all rainwater captured on site	Amount of rainwater captured (kL)	15.1	13.5
		Amount of captured rainwater used (kL)	15.1	13.5
	Relative consumption of water—per employee	Amount of total water used (kL) per employee	31.6	32.5
	<b>Water rating</b>	NABERS water rating (1–6)	2 stars	1.5 stars
	<b>Steps taken to reduce effect</b> <p>ASIO consumes fresh water from the public water network, artesian water sources and rainfall, for cooling, fire safety and staff use purposes.</p>	<b>Measures to review and improve reducing the effect</b> <p>Captured stormwater for irrigation and toilet flushing, reducing reliance on potable and bore water</p>		

# Appendix I: report of the Independent Reviewer of Adverse Security Assessments

The Independent Reviewer of Adverse Security Assessments, Robert Cornall AO, conducts an independent advisory review of ASIO adverse security assessments (ASAs) furnished to the Department of Home Affairs in respect of eligible persons being persons who:

- remain in immigration detention, and
- have been found by Home Affairs to be owed protection obligations under international law, and
- are ineligible for a permanent protection visa, or have had their permanent protection visa cancelled, because they are the subject of the ASA.

The Independent Reviewer's terms of reference and other relevant information are available at [www.ag.gov.au/asareview](http://www.ag.gov.au/asareview).

The Reviewer undertakes a primary review of each adverse security assessment (ASA) which comes within the terms of reference and subsequent periodic reviews every 12 months thereafter while the person remains in detention and ineligible to hold a visa because they are subject to the ASA.

On 1 July 2019, the Independent Reviewer had two adverse security assessments under consideration and another three ASAs were referred to the Reviewer during the course of the year. The Reviewer commenced a primary review in each of the five cases and three reviews were completed before 30 June 2020.

In those three cases, the Reviewer examined all the material ASIO relied on in making the adverse assessment as well as other relevant material including submissions and representations made by the eligible person. In addition, the Reviewer conducted an interview with the eligible person and their legal representative.

The Reviewer also took into account the overall security environment, which is informed by ASIO's contemporary assessment of security threats, and any changes to the person's circumstances or ideology during their time in immigration detention.

In the first two completed reviews, the Reviewer found the ASA was an appropriate outcome. However, in each of those cases, the Reviewer recommended that, when ASIO conducts an internal review of the ASA, it gives further consideration to some specified circumstances which may influence the outcome of ASIO's review.

In the third completed primary review, the Reviewer found that the ASA was an appropriate outcome.

Each of those three adverse assessments will, unless it is withdrawn, be subject to a periodic review during 2020–21.

Where it appears the Reviewer may arrive at an opinion that the ASA was not an appropriate outcome, the Reviewer is required to provide the Director-General of Security with a reasonable opportunity to comment before finalising that opinion.

In the fourth case, the Reviewer commenced a primary review of the ASA but, before proceeding further, raised some issues with ASIO in accordance with the terms of reference. The Director-General advised the Reviewer to put the review on hold while ASIO considered the matter further. Following that consideration, the ASA was withdrawn on 8 July 2020 and replaced a qualified security assessment (which falls outside the terms of reference). The Independent Reviewer terminated the incomplete primary review and advised the eligible person's solicitor accordingly.

In the fifth case, the Reviewer commenced a primary review and conducted an interview with the eligible person and their legal representative before the Director-General asked for the review to be suspended while ASIO undertook more inquiries. On 16 July 2020, ASIO withdrew the existing adverse security assessment in respect of the eligible person and furnished another ASA in its place. Accordingly, the Reviewer terminated the incomplete primary review and commenced a primary review of the new adverse assessment.

The Independent Reviewer's two year appointment is due to expire on 26 March 2021.

# Appendix J: report on use of questioning warrants and questioning and detention warrants

ASIO is required under section 94 of the ASIO Act to provide in its annual report details of its use of questioning warrants and question and detention warrants during this reporting period. The details are provided in the following table.

Subsection	Description	2017–18	2018–19	2019–20
94(1)(a)	The total number of requests made under Division 3 of Part III to issuing authorities for the issue of warrants under that division during this reporting period	0	0	0
94(1)(b)	The total number of warrants issued under that division during this reporting period	0	0	0
94(1)(c)	The total number of warrants issued under section 34E during this reporting period	0	0	0
94(1)(d)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued under section 34E, and the total of all those hours for all those persons, during this reporting period	0	0	0
94(1)(e)	The total number of warrants issued under section 34G during this reporting period	0	0	0
94(1)(f)(i)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued under section 34G during this reporting period	0	0	0
94(1)(f)(ii)	The number of hours each person spent in detention under such a warrant during this reporting period	0	0	0
94(1)(f)(iii)	The total of all those hours for all those persons during this reporting period	0	0	0
94(1)(g)	The number of times each prescribed authority had persons appear for questioning before them under warrants issued during this reporting period	0	0	0

# List of annual report requirements under schedule 2 of the Public Governance, Performance and Accountability Rule

Below is the table set out in Schedule 2 of the Public Governance, Performance and Accountability (PGPA) Rule. Subsection 17AJ(d) of the Rule requires annual reports of Australian Government entities to include this table as an aid for accessibility.

PGPA Rule reference	Description	Requirement	Part of this report
<b>17AD(g)</b>	<b>Letter of transmittal</b>		
17AI	A copy of the letter of transmittal signed and dated by an accountable authority on the date final text was approved, with a statement that the report has been prepared in accordance with section 46 of the Act and any enabling legislation that specifies additional requirements in relation to the annual report.	Mandatory	Letter of transmittal
<b>17AD(h)</b>	<b>Aids to access</b>		
17AJ(a)	Table of contents.	Mandatory	Preliminaries
17AJ(b)	Alphabetical index.	Mandatory	Appendices
17AJ(c)	Glossary of abbreviations and acronyms.	Mandatory	Appendices
17AJ(d)	List of requirements.	Mandatory	Appendices
17AJ(e)	Details of contact officer.	Mandatory	Preliminaries
17AJ(f)	Entity's website address.	Mandatory	Preliminaries
17AJ(g)	Electronic address of report.	Mandatory	Preliminaries
<b>17AD(a)</b>	<b>Review by an accountable authority</b>		
17AD(a)	A review by the entity's accountable authority.	Mandatory	Part 1
<b>17AD(b)</b>	<b>Overview of the entity</b>		
17AE(1)(a)(i)	A description of the role and functions of the entity.	Mandatory	Part 2
17AE(1)(a)(ii)	A description of the organisational structure of the entity.	Mandatory	Part 2
17AE(1)(a)(iii)	A description of the outcomes and programmes administered by the entity.	Mandatory	Part 2
17AE(1)(a)(iv)	A description of the purposes of the entity as included in ASIO's corporate plan.	Mandatory	Part 2

PGPA Rule reference	Description	Requirement	Part of this report
17AE(1)(aa)(i)	Name of the accountable authority or each member of the accountable authority.	Mandatory	Part 5
17AE(1)(aa)(ii)	Position title of the accountable authority or each member of the accountable authority.	Mandatory	Part 5
17AE(1)(aa)(iii)	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	Part 5
17AE(1)(b)	An outline of the structure of the portfolio of the entity.	Mandatory for portfolio departments	Not applicable
17AE(2)	Where the outcomes and programs administered by the entity differ from any Portfolio Budget Statement, Portfolio Additional Estimates Statement or other portfolio estimates statement that was prepared for the entity for the period, include details of variation and reasons for change.	If applicable, mandatory	Not applicable
<b>17AD(c)</b>	<b>Report on the performance of the entity</b>		
	<b><i>Annual performance statements</i></b>		
17AD(c)(i); 16F	Annual performance statement in accordance with paragraph 39(1)(b) of the PGPA Act and section 16F of the Rule.	Mandatory	Part 4
<b>17AD(c)(ii)</b>	<b><i>Report on financial performance</i></b>		
17AF(1)(a)	A discussion and analysis of the entity's financial performance.	Mandatory	Part 4
17AF(1)(b)	A table summarising the entity's total resources and total payments of the entity.	Mandatory	Appendices A and B
17AF(2)	If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes, including: the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken in relation to the loss; and any matter or circumstances that it can reasonably be anticipated will have a significant impact on the entity's future operation or financial results.	If applicable, mandatory	Not applicable
<b>17AD(d)</b>	<b>Management and accountability</b>		
	<b><i>Corporate governance</i></b>		
17AG(2)(a)	Information on compliance with section 10 (fraud systems).	Mandatory	Letter of transmittal and Part 5
17AG(2)(b)(i)	Certification by an accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	Letter of transmittal

PGPA Rule reference	Description	Requirement	Part of this report
17AG(2)(b)(ii)	A certification by accountable authority that appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place.	Mandatory	Letter of transmittal
17AG(2)(b)(iii)	A certification by an accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity.	Mandatory	Letter of transmittal
17AG(2)(c)	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance.	Mandatory	Part 5
17AG(2)(d)–(e)	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to non-compliance with Finance law and action taken to remedy non-compliance.	If applicable, mandatory	Not applicable
<b>Audit Committee</b>			
17AG(2A)(a)	A direct electronic address of the charter determining the functions of the entity's audit committee.	Mandatory	Exempt
17AG(2A)(b)	The name of each member of the entity's audit committee.	Mandatory	Exempt
17AG(2A)(c)	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	Part 5
17AG(2A)(d)	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	Part 5
17AG(2A)(e)	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	Part 5
<b>External scrutiny</b>			
17AG(3)	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	Part 5
17AG(3)(a)	Information on judicial decisions and decisions of administrative tribunals and by the Australian Information Commissioner that may have a significant effect on the operations of the entity.	If applicable, mandatory	Part 5
17AG(3)(b)	Information on any reports on operations of the entity by the Auditor General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, mandatory	Not applicable
17AG(3)(c)	Information on any capability reviews on the entity that were released during the period.	If applicable, mandatory	Not applicable

PGPA Rule reference	Description	Requirement	Part of this report
<b>Management of human resources</b>			
17AG(4)(a)	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	Part 5
17AG(4)(a)(a)	Statistics on the entity's employees on an ongoing and non-ongoing basis; including the following: <ul style="list-style-type: none"> <li>a. statistics on full-time employees;</li> <li>b. statistics on part-time employees;</li> <li>c. statistics on gender;</li> <li>d. statistics on staff location; and</li> <li>e. statistics on employees who identify as Indigenous.</li> </ul>	Mandatory	Appendix C
17AG(4)(b)	Statistics on the entity's APS employees on an ongoing and non-ongoing basis; including the following: <ul style="list-style-type: none"> <li>■ statistics on staffing classification;</li> <li>■ statistics on full-time employees;</li> <li>■ statistics on part-time employees;</li> <li>■ statistics on gender;</li> <li>■ statistics on staff location; and</li> <li>■ statistics on employees who identify as indigenous.</li> </ul>	Mandatory	Not applicable
17AG(4)(c)	Information on any enterprise agreements, individual flexibility arrangements, Australian workplace agreements, common law contracts and determinations under subsection 24(1) of the <i>Public Service Act 1999</i> .	Mandatory	Part 5
17AG(4)(c)(i)	Information on the number of SES and non SES employees covered by agreements etc. identified in paragraph 17AG(4)(c).	Mandatory	Appendix C
17AG(4)(c)(ii)	The salary ranges available for APS employees by classification level.	Mandatory	Appendix D
17AG(4)(c)(iii)	A description of non-salary benefits provided to employees.	Mandatory	Not applicable
17AG(4)(d)(i)	Information on the number of employees at each classification level who received performance pay.	If applicable, mandatory	Not applicable
17AG(4)(d)(ii)	Information on aggregate amounts of performance pay at each classification level.	If applicable, mandatory	Not applicable



PGPA Rule reference	Description	Requirement	Part of this report
17AG(4)(d)(iii)	Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, mandatory	Not applicable
17AG(4)(d)(iv)	Information on aggregate amount of performance payments.	If applicable, mandatory	Not applicable
<b>Assets management</b>			
17AG(5)	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, mandatory	Not applicable
<b>Purchasing</b>			
17AG(6)	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	Part 5
<b>Consultants</b>			
17AG(7)(a)	A summary statement detailing the number of new contracts engaging consultants entered into during the period; the total actual expenditure on all new consultancy contracts entered into during the period (inclusive of GST); the number of ongoing consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST).	Mandatory	Part 5
17AG(7)(b)	A statement that ' <i>During [reporting period], [specified number] new consultancy contracts were entered into involving total actual expenditure of \$[specified million]. In addition, [specified number] ongoing consultancy contracts were active during the period, involving total actual expenditure of \$[specified million]</i> '.	Mandatory	Part 5
17AG(7)(c)	A summary of the policies and procedures for selecting and engaging consultants and the main categories of purposes for which consultants were selected and engaged.	Mandatory	Part 5
17AG(7)(d)	A statement that, ' <i>Annual reports contain information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website</i> '.	Mandatory	Part 5
<b>Australian National Audit Office access clauses</b>			
17AG(8)	If an entity entered into a contract with a value of more than \$100 000 (inclusive of GST) and the contract did not provide the Auditor-General with access to the contractor's premises, the report must include the name of the contractor, purpose and value of the contract, and the reason why a clause allowing access was not included in the contract.	If applicable, mandatory	Not applicable

PGPA Rule reference	Description	Requirement	Part of this report
<b>Exempt contracts</b>			
17AG(9)	If an entity entered into a contract or there is a standing offer with a value greater than \$10 000 (inclusive of GST) which has been exempted from being published in AusTender because it would disclose exempt matters under the Freedom of Information Act (FOI Act), the annual report must include a statement that the contract or standing offer has been exempted, and the value of the contract or standing offer, to the extent that doing so does not disclose the exempt matters.	If applicable, mandatory	Part 5
<b>Small business</b>			
17AG(10)(a)	A statement that, ' <i>[Name of entity] supports small business participation in the Commonwealth Government procurement market. Small and Medium Enterprises (SME) and Small Enterprise participation statistics are available on the Department of Finance's website.</i>	Mandatory	Part 5
17AG(10)(b)	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	Part 5
17AG(10)(c)	If the entity is considered by the Department administered by the Finance Minister as material in nature—a statement that, ' <i>[Name of entity] recognises the importance of ensuring that small businesses are paid on time. The results of the Survey of Australian Government Payments to Small Business are available on Treasury's website.</i>	If applicable, mandatory	Part 5
<b>Financial statements</b>			
17AD(e)	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	Part 6
<b>Executive remuneration</b>			
17AD(da)	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 2-3 of the Rule.	Mandatory	Appendix C
<b>17AD(f) Other mandatory information</b>			
17AH(1)(a)(i)	If the entity conducted advertising campaigns, a statement that ' <i>During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity's website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website.</i>	If applicable, mandatory	Part 5

PGPA Rule reference	Description	Requirement	Part of this report
17AH(1)(a)(ii)	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, mandatory	Not applicable
17AH(1)(b)	A statement that, 'Information on grants awarded to [name of entity] during [reporting period] is available at [address of entity's website]'.	If applicable, mandatory	Not applicable
17AH(1)(c)	Outline of mechanisms of disability reporting, including reference to a website for further information.	Mandatory	Part 5
17AH(1)(d)	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	Mandatory	Not applicable (FOI exempt)
17AH(1)(e)	Correction of material errors in the previous annual report.	If applicable, mandatory	Not applicable
17AH(2)	Information required by other legislation.	Mandatory	Appendices

# List of annual report requirements under other legislation

ASIO is required by section 94 of the ASIO Act to include in its annual report, details on its use of questioning warrants and questioning and detention warrants; special intelligence operation authorities; authorisations for access to telecommunications data; technical assistance requests, technical assistance notices and technical capability notices; and use of special powers under warrant.

Requirement	Refer to
Statement on questioning warrants and questioning and detention warrants	Appendix J
Statement on special intelligence operation authorities	Appendix K
Statement on authorisations for access to telecommunications data	Appendix L
Statement on use of technical assistance requests, technical assistance notices and technical capability notices	Appendix M
Statement on use of special powers under warrant	Appendix N

To comply with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance Performance and Accountability Act 2013*, appendices K, L, M and N have been deleted from the version of the annual report tabled in parliament to avoid prejudice to ASIO's activities.

# Abbreviations and short forms

## A

AASB—Australian Accounting Standards Board

AASB 9—Australian Accounting Standards Board Standard ‘Financial Instruments’

AASB 119—Australian Accounting Standards Board Standard ‘Employee Benefits’

AAT—Administrative Appeals Tribunal

ACIC—Australian Criminal Intelligence Commission

ACSC—Australian Cyber Security Centre

AE—ASIO employee

AEE—ASIO executive employee

AFP—Australian Federal Police

AGSVA—Australian Government Security Vetting Agency

ANZCTC—Australia-New Zealand Counter-Terrorism Committee

AO—Officer of the Order of Australia

APS—Australian Public Service

ASA—adverse security assessment

ASD—Australian Signals Directorate

ASIC—Aviation Security Identification Card

ASIO Act—*Australian Security Intelligence Organisation Act 1979*

ASIO—Australian Security Intelligence Organisation

ASIS—Australian Secret Intelligence Service

## B

## C

CFIC—Counter Foreign Interference Coordinator

CFITF—Counter Foreign Interference Taskforce

CMT—Crisis Management Team

CPR—Commonwealth Procurement Rules

COVID-19—coronavirus disease 2019

CSC—Conspicuous Service Cross

## D

DFAT—Department of Foreign Affairs and Trade

DSC—Distinguished Service Cross

## E

EFI—espionage and foreign interference

EAP—employee assistance program

eLearning—ASIO’s intranet-based learning software program

## F

FIRB—Foreign Investment Review Board

FIS—foreign intelligence services

## G

GST—Goods and Services Tax

## H

HaDA—Harassment and Discrimination Advisor

Home Affairs—Department of Home Affairs

HR—human resources

HRTTO scheme—High Risk Terrorist Offenders scheme

HUMINT—human intelligence

## I

IE—intelligence employees

IGIS—Inspector-General of Intelligence and Security

INSLM—Independent National Security Legislation Monitor

ISIL—Islamic State of Iraq and the Levant

ITE—information technology employee

## J

JCTT—Joint Counter-Terrorism Team/s

## K

kWh—kilowatt hour

## M

MSIC—Maritime Security Identification Card

## N

NABERS—National Australian Built Environment Rating System

NIC—National Intelligence Community

NV—‘Negative vetting’ security clearance

## O

Office of National Intelligence

Outreach—(formerly Business Government and Liaison Unit (BGLU))

## P

PBS—Portfolio Budget Statement

PGPA Act—*Public Governance, Performance and Accountability Act 2013*

PGPA Rule—Public Governance, Performance and Accountability Rule

PII—potential irregular immigrants

PJCIS—Parliamentary Joint Committee on Intelligence and Security

PSPF—Protective Security Policy Framework

PV—Top Secret ‘positive vetting’ security clearance

## R

RAP—Reconciliation Action Plan

## S

SCEC—Security Construction and Equipment Committee

SES—Senior Executive Service

SIE(E)—specialist intelligence employee (engineer)

SITE—senior information technology employee

SME—small and medium enterprises

STEM—science, technology, engineering and mechanics

## T

T20—Twenty20 cricket series

TL&P—tenant light and power

TOLA Act—*Telecommunications and Other Legislation Amendment Act 2018*

TSCM—Technical Surveillance Countermeasures

TSSR—Telecommunication Sector Security Reforms

## U

## V

## W

## X

## Y

## Z

## Glossary

*adverse security assessment*—ASIO recommends that a particular prescribed administrative action be taken or not taken which would be prejudicial to the interests of the person, such as the refusal of a visa or cancellation of a passport.

*communal violence*—violence between different groups or individuals in the Australian community that endangers the peace, order or good government of the Commonwealth.

*espionage*—the theft of Australian information or capability by individuals either acting on behalf of a foreign power or with the intent of providing information to a foreign power in order to provide that foreign power with an advantage.

*foreign fighters*—Australians who have participated in foreign conflicts or undertaken training with extremist groups overseas.

*foreign interference*—activities relating to Australia that are conducted by, or on behalf of, a foreign power; are directed or subsidised by a foreign power; or are undertaken in active collaboration with a foreign power. These activities:

- a. involve a threat to any person; or
- b. are clandestine or deceptive and:
  - are conducted for intelligence purposes;
  - are conducted for the purpose of affecting political or governmental processes; or
  - are otherwise detrimental to the interests of Australia.

*foreign power*—a foreign government, or an entity that is directed or controlled by a foreign government or governments, or a foreign political organisation.

*investigation*—the processes involved in collecting, correlating and evaluating information on known harmful activities and emerging security risks. The purpose of ASIO's security investigations is to develop insights that inform government decision-making and enable preventative action, including by partner agencies.

*jihadist*—commonly used as a noun to refer to a person involved in violent jihad.

*malicious insiders*—trusted employees and contractors who deliberately breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

*non-prejudicial assessment*—ASIO does not have security concerns about the proposed action.

*qualified security assessment*—ASIO does not make a prejudicial recommendation but does communicate information, an opinion or advice that is, or could be, prejudicial to the interests of the person in relation to the contemplated prescribed administrative action.



*radicalisation*—the process by which an individual’s beliefs move from mainstream views (those commonly accepted by the majority within a society) towards more marginal views (those less widely accepted or not accepted by the majority within a society). Radicalisation occurs across a spectrum, and some individuals may become radicalised sufficiently to advocate or use violence to effect societal or political change.

*terrorism*—a tactic that can be employed by any group or individual determined to use violence to achieve or advance a political goal.

*violent extremism*—any ideology or world view that is advanced through the use of violence; violent extremism is unlawful.

# Index

## A

Aboriginal and Torres Strait Islander 11

Administrative Appeals Tribunal (AAT) 65, 139

adverse security assessment 18, 49, 62, 65, 128, 129, 139, 142

advertising 71, 73, 124, 136, 137

Afghanistan 20

al-Qa'ida 17, 19, 20, 21, 33, 34

al-Qa'ida in the Indian Subcontinent 33

ASIO employees 65, 120, 121, 126

ASIO Ombudsman 68

ASIO's Corporate Plan 30

ASIO-T4 52

Attorney-General 73

Audit and Risk Committee 57, 61, 63, 64, 69, 70

AusCheck 34

AusTender 69, 135, 136

Australia-based family and associates 34

Australia-based foreign national 4, 40

Australian Border Force 32

*Australian Citizenship Act 2007* (Citizenship Act) 60

Australian Citizenship Amendment (Citizenship Cessation) Bill 2019 60

Australia-New Zealand Counter-Terrorism Committee (ANZCTC) 37, 139

Australian Federal Police (AFP) 32, 43, 45, 139

Australian Government Security Vetting Agency (AGSVA) 40, 44, 139

Australian Public Service 71, 139

Australian Secret Intelligence Service (ASIS) 43, 139

*Australian Security Intelligence Organisation Act 1979* 9, 73, 113, 139

Australian Signals Directorate (ASD) 38, 41, 43, 139

Australia's security environment 17, 53

aviation 33

Aviation Security Identification Cards (ASICs) 34

## B

Ben Chifley Building 68

border integrity 9, 30, 45, 48, 49

border security 47

budget 54, 83, 84, 85, 86, 87, 88, 100, 101, 105, 106, 107, 111, 112

Burgess, Mike 5, 10, 29, 81

Burkina Faso 21

business continuity 59

## C

Chief Transformation Officer 114

Citizenship Act 60

clearances 40, 65

Code of Conduct 123

Comcare 65, 122

Commonwealth Disability Strategy 71

Commonwealth Fraud Control Framework 64

Commonwealth Ombudsman 133

Commonwealth Procurement Rules 69, 135, 139

communal violence 22, 142

consultancy contracts 69, 135

corporate governance 57, 132

counter-espionage and foreign interference v, 30, 39, 56, 59

counter-foreign interference 25, 43

Counter Foreign Interference Taskforce (CFITF) 39, 43, 139

countering espionage, foreign interference, sabotage and malicious insiders 9

counter-terrorism v, 3, 18, 21, 30, 32, 33, 36, 37, 62

counter-terrorism and counter-espionage and foreign interference 56, 59

counter-terrorism investigative subjects 3, 18

COVID-19 v, 3, 17, 18, 19, 20, 21, 24, 31, 35, 37, 39, 41, 46, 48, 50, 52, 53, 54, 56, 59, 67, 68, 72, 100, 105, 106, 122, 124, 139

Crisis Management Team (CMT) 59, 139

critical infrastructure 25, 33

crowded places 19

cyber espionage 23, 39

## D

Defence 23, 24, 41, 44

defence industry 38, 44, 51

deficit 54, 85, 101

Departmental Capital Budget 54

Department of Finance 70, 71, 90, 105, 114, 115, 116, 124, 136

Department of Foreign Affairs and Trade (DFAT) 33, 44, 45, 100, 139

Department of Home Affairs iii, 41, 45, 49, 60, 128, 140, 145, 146

Department of Treasury 41

depreciation 54, 95, 96, 97, 101, 105, 106, 112

detention 62, 73, 128, 130, 138

detention warrants 73, 130, 138

disability 71, 137

disruption 4, 18, 20, 22, 25, 32, 39, 40, 59, 105

diversity and inclusion 67

Diversity and Inclusion Strategy 2018–20 67

diversity networks 68

## E

Egypt 21

espionage iv, v, vi, 2, 4, 9, 23, 24, 25, 30, 39, 40, 42, 43, 56, 59, 139, 142, 144, 145

espionage and foreign interference iv, v, 2, 4, 23, 24, 30, 39, 42, 56, 59, 139, 145

Europe 19

Executive Committee 5, 57, 58, 63, 104, 113

explosives 19

external partners/stakeholders 31, 35, 36, 40, 41, 44, 45, 46, 47, 48, 50, 59, 66, 145, 147

external scrutiny 57, 60, 133

extreme right-wing 3, 17, 18, 33, 35

## F

Federal and High Court 66

federal election 60

financial statements 77, 81, 89

foreign actors 25

foreign fighters 19, 142

foreign intelligence operation 40, 42, 145

foreign intelligence services (FIS) 23, 24, 25, 39, 40, 42, 43, 139

foreign interference 4, 25

foreign investment 25, 41, 139

Foreign Investment Review Board (FIRB) 25, 41

foreign power 142

foreign states v, 16, 23

fraud risk assessment 64

full-time employees 134

## G

gender 68, 118, 119, 134

Goods and Services Tax (GST) 69, 87, 91, 94, 101, 135, 136, 139

governance 29, 57, 63, 64, 70, 81, 89, 111, 112, 113, 114, 118, 119, 120, 121, 131, 138, 140

graduate programs 124

## I

immigration detention 62, 128

Independent National Security Legislation Monitor (INSLM) 5, 62, 140

Independent Reviewer 62, 128, 129

Indigenous 121, 134

Indonesia 20

industry 4, 9, 23, 24, 31, 35, 37, 38, 41, 43, 44, 47, 50, 51, 53

Inspector-General of Intelligence and Security (IGIS) 5, 9, 61, 140

intelligence and security reports 35

intelligence priorities 36

international partners 37, 43, 44, 48, 51

Iraq 3, 20, 33

irregular maritime ventures 21

irregular migration 21, 48

Islamic State of Iraq and the Levant (ISIL) 3, 17, 18, 19, 20, 21, 34, 140

IS-Libya 33

Israel 21

IS-Sinai 33

## J

Joint Counter-Terrorism Teams (JCTT) 32, 33, 34, 140

Joint Standing Committee on Electoral Matters 60

## L

Leader of the Opposition 73

Leadership Charter 123

Lewis AO, DSC, CSC, Mr Duncan 10, 29

## M

Mali-based 21

Maritime Security Identification Cards (MSICs) 34, 140

Middle East 20, 21

Minister for Finance 73, 138

Mozambique 21

## N

National Australian Built Environment Rating System (NABERS) 125, 126, 127, 140

National Counter-Terrorism Strategy 37

National Disability Strategy 2010–20 71

National Intelligence Community (NIC) 36, 40, 43, 140

*National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* 53

national terrorism threat level v, 16, 17

neo-Nazis 17

North America 19

## O

organisational structure 12

outreach 43, 124

Outreach 24, 140

oversight 3, 5, 9, 58, 60, 63

## P

Pakistan 20

Palestinian Territories 21

Parliamentary Joint Committee on Intelligence and Security (PJCIS) 5, 60, 69, 70, 73, 140

people smuggling 30, 45, 49

people with a disability 71

permanent protection visa 128

personnel security assessments 40, 42, 44

Portfolio Budget Statement (PBS) 31, 32, 35, 37, 39, 41, 43, 45, 47, 48, 50, 51, 105, 132, 140, 147

Positive Vetting (PV) clearances 40, 140

private sector/private sector stakeholders 50, 59

propaganda 17, 19, 20, 35

prosecution 32

protective security advice 9, 30, 43, 50, 52

*Public Governance, Performance and Accountability Act 2013* (PGPA Act) 29, 57, 63, 64, 81, 89, 100, 111, 112, 114, 118, 119, 120, 121, 138, 140, 147

public interest disclosure 123

## Q

qualified personnel security assessments 40

qualified security assessment 129, 142

questioning and detention warrants 73, 130, 138

questioning warrants 73, 130, 138

## R

right-wing extremism 18

risk management 122

## S

sabotage 18

Saudi Arabia 21

science, technology, engineering and maths (STEM) 11, 124, 140

Security and Compliance Committee 57, 58

security environment 3, 11, 19, 20, 25, 36, 58, 62, 128

security managers guides 50, 52

security risks 24, 31, 40, 45, 142

security zone briefings 38

security zones 51

Security Zones course 51

Senate estimates 61

Senate Legal and Constitutional Affairs Committee 61

Senior Executive Service (SES) employees 113, 117, 118, 119, 134, 140

small and medium enterprises (SME) 70, 136, 140

small business 70, 136

South Asia 20

special intelligence operation authorisations/authorities 73, 138

Sunni Islamic extremism v, 3, 16, 17

surplus 54, 83, 86, 101

Syria 3, 20, 21, 33, 34, 147

## T

technical assistance requests 73, 138, 147

Technical Surveillance Countermeasures (TSCM) 50, 141

telecommunications sector 25

Temporary Exclusion Orders 33

terrorism disruption 18

terrorism laws 18, 33  
terrorism offences 18, 32, 33  
terrorist act 18, 32, 33  
terrorist attack 3, 17, 19  
terrorist groups 18, 21  
terrorist organisations 33, 60  
terrorist targets 19  
terrorist threat 19, 20, 21, 33  
tertiary sector 39  
training courses 37, 52  
Treasury 136  
Turkey 21

## U

universities 23, 43, 124  
University Foreign Interference Taskforce 43

## V

violent protest 22  
visa assessments 46, 48  
visa security assessments 45, 47, 148

## W

warrants 73, 130, 138  
waste 125, 126, 127  
weapons 19  
weapons and tactics 19, 34  
workforce iv, 5, 10, 59, 67, 68, 71, 118, 122, 124  
work health and safety 73, 122  
*Work Health and Safety Act 2011* 73, 122  
workplace agreement 67

## Y

Yemen 21

## Z

zero tolerance 64  
Zone 5 facilities 51, 52





*asio.gov.au*