



Australian Government
Australian Security
Intelligence Organisation

ANNUAL REPORT 2021-22



Securing Australia—protecting its people

Aids to access

© Commonwealth of Australia 2022

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).

Report a threat

National Security Hotline 1800 123 400
hotline@nationalsecurity.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. The annual report can also be viewed at 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

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.

An aerial photograph of a city street with a teal overlay. Several people are walking in different directions. A dog on a leash is visible in the lower right. The text 'ANNUAL REPORT' is in white, and '2021-22' is in a light teal color.

ANNUAL REPORT

2021-22



18* October 2022
Ref: A22388322

The Hon. Clare O'Neil, MP
Minister for Home Affairs
Parliament House
CANBERRA ACT 2600

Dear Minister,

ASIO Annual Report 2021-22

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 2021-22.

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 avoid prejudice to security and to ensure compliance with section 94 of the ASIO Act, I have provided you advice to remove statements required under subsections 94(2A), 94(2B), 94(2BA), 94(2BC), 94(2BD) and 94(2BBA) of the ASIO Act from the annual report tabled in Parliament, under section 94(5) of the ASIO Act. To avoid prejudice to designated activities of ASIO and to ensure compliance with the PGPA Act, I have used the determination made by the Minister for Finance under section 105D of the PGPA Act to remove statements required under PGPA Rule subsections 17(AD)(e), 17AG(2A)(a-e) and 17AG(4)(aa)(iv) from the annual report tabled in Parliament. These statements have been separately provided to you and, as required by the ASIO Act, will be provided to the Leader of the Opposition. A copy of the classified appendices will also be provided to the Parliamentary Joint Committee on Intelligence and Security, the Inspector-General of Intelligence and Security and the Independent National Security Legislation Monitor.

As required by subsection 17AG(2)(b)(i-iii) 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

Contents

1	DIRECTOR-GENERAL'S REVIEW	1
2	OVERVIEW OF ASIO	9
	Our most important asset is our people	13
	Organisational structure	14
3	AUSTRALIA'S SECURITY ENVIRONMENT AND OUTLOOK	17
4	REPORT ON PERFORMANCE	27
	Annual performance statement 2021–22	29
	Summary of results	31
	Reporting framework	32
	ASIO's purpose	33
	Performance measures	35
	Performance methodology	36
	Analysis of performance	39
	Counter-terrorism	42
	Counter-espionage and foreign interference	49
	Border security	57
	ASIO capability program	61
	Risk and compliance	65
	Report on financial performance	67

5	MANAGEMENT AND ACCOUNTABILITY	69
	Corporate governance	71
	ASIO's response to COVID-19	73
	External scrutiny	74
	Compliance	76
	Significant legal matters affecting ASIO's business	78
	Management of human resources	79
	Other mandatory information	86
6	FINANCIAL INFORMATION	91
A	APPENDICES	113
	Appendix A: ASIO resource statement	115
	Appendix B: expenses by outcomes	116
	Appendix C: report of the Independent Reviewer of Adverse Security Assessments	117
	Appendix D: executive remuneration	121
	Appendix E: ASIO's salary classification structure	125
	Appendix F: workforce statistics by headcount	126
	Appendix G: recruitment, advertising and market research	129
	Appendix H: work health and safety	130
	Appendix I: ecologically sustainable development and environmental performance	132
	Appendix J: report on use of questioning warrants	135
	Appendix K: correction of material errors in previous annual report	136
	List of annual report requirements under schedule 2 of the Public Governance, Performance and Accountability Rule	140
	List of annual report requirements under the ASIO Act	147
	Abbreviations and short forms	148
	Glossary	150
	Index	151

1





1

DIRECTOR-GENERAL'S REVIEW



Director-General's review

Australia's security outlook remains complex, challenging and changing.

Complex, because the threat environment is increasingly volatile and shaped by diverse drivers that range from geopolitical to technical, ideological to environmental.

Challenging, because Australia is being targeted by sophisticated foreign adversaries that are effectively unconstrained by resources, ethics or laws. Encryption is making threats to life from lone actors or small groups more difficult to detect.

Changing, because threats are increasingly intersecting, emerging from new places and blurring the distinctions between ASIO's legislated responsibilities.

Threats to our way of life

Espionage and foreign interference has supplanted terrorism as our principal security concern.

Multiple countries are aggressively seeking information about Australia's strategic capabilities, economic and policy priorities, world-class research and development, and defence technologies.

We anticipate hostile foreign powers and their proxies will be particularly interested in obtaining information on AUKUS, the Quad and their associated initiatives.

While cyber remains the most pervasive vector for espionage, the re-opening of international borders will make it easier for foreign intelligence services to gather intelligence in person, on location in Australia.

Multiple foreign governments are determined to interfere in Australia's democracy and undermine our sovereignty.

We see this primarily manifested in the harassment of diaspora communities, and attempts to shape political and business decision-making to the foreign governments' advantage.

These attempts are occurring in all states and territories, at all levels of government, on all sides of politics and in the private sector.

Threats to life

Threats to life will always be a priority for ASIO.

The most likely terrorist attack scenario in Australia continues to be a lone actor attack without warning and using a rudimentary and readily available weapon such as a knife or vehicle.

While ASIO's overall counter-terrorism caseload is moderating, the threats posed by religiously motivated violent extremists and ideologically motivated violent extremists remain real. I remain concerned by the number of young Australians who are being radicalised and recruited by both cohorts.

Specific-issue motivated violent extremism grew during COVID-19 and its associated lockdowns. Angry, alienated individuals and groups were being driven by a range of grievances, including anti-vaccination agendas, conspiracy theories and anti-government sovereign citizen beliefs. In most cases, these grievances were expressed peacefully, but in some cases protesters advocated the use of violence, and in a smaller number of cases, they used violence—the factors that trigger ASIO's interest.

Sabotage

ASIO anticipates malign foreign powers will consider using sabotage to coerce, disrupt or retaliate during times of escalating geopolitical tensions.

Pre-positioning malicious code in Australia's critical infrastructure is the most likely means.

ASIO's response

Notwithstanding this complex, challenging and changing environment, ASIO remains well placed to advance our mission of protecting Australia and Australians from threats to their security.

In 2021–22, working with our law enforcement partners, our targeted investigations led to multiple disruptions, arrests and convictions.

We are stepping up our work with government and industry to harden the environment against espionage and foreign interference threats. According to our annual survey, ASIO's stakeholders embraced these efforts in the reporting period, and noted improvements in our willingness to engage. To build on this, I established a new Influence and Impact Committee, chaired by my Principal Advisor, to provide assurance that our advice is reaching the right people, the right way, at the right time.

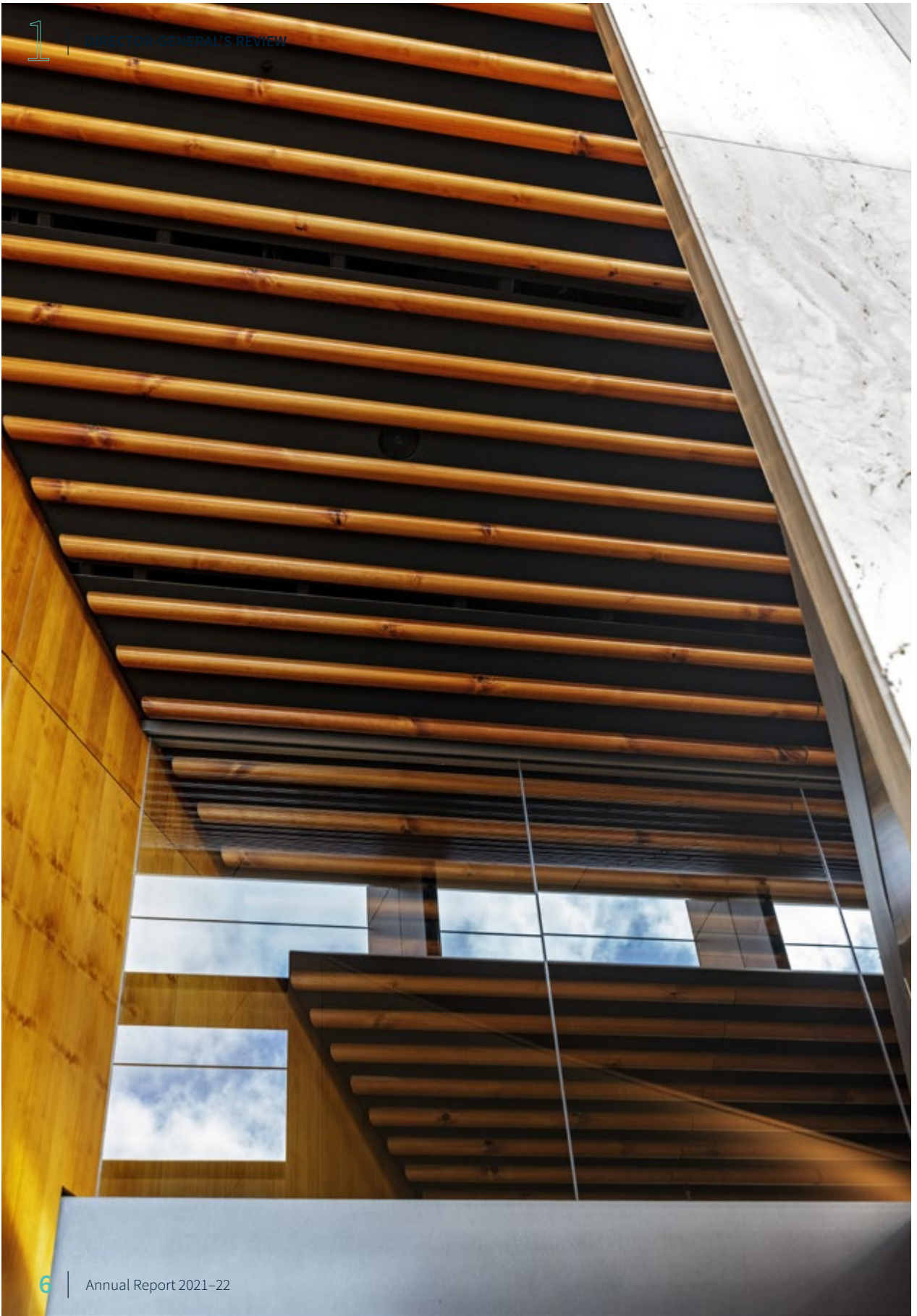
In 2022, ASIO launched its 'Prying Minds' campaign to raise awareness of the threat foreign spies and proxies pose to Australia's defence industry. Our awareness raising reached thousands of employees in defence industry across engineering, design, manufacturing, program management, logistics and ICT support services. ASIO also established a new secure online portal, 'NITRO'—*Notifiable Incidents, Threats and Reportable Observations*—to enable non-clearance holders to report concerns about espionage, insider threats and foreign interference directly to ASIO.

ASIO's most important asset is its people. We are developing, adapting and adopting new ways of working and thinking to stay ahead of Australia's adversaries, and rapidly evolving technology.

Following a significant government investment, our new capability uplift program will enhance our ability to 'connect the dots' through a human-led, data-driven, technology-enabled approach to threat detection.

In the reporting period, ASIO made significant progress designing and delivering the foundations of the program.

I am particularly pleased with the new relationships and supply chains that are being developed with the technology sector. We will work with Australian companies to leverage emerging technologies and ensure our capabilities are sharper than cutting edge.



The scale and sophistication of the threats facing Australia demands robust and resilient security settings. Vetting is a key component of this; only appropriately cleared people should have access to our nation's most sensitive secrets.

In May, I appointed Ewan Macmillan as Deputy Director-General Vetting Service Delivery. Ewan is leading the development and implementation of a suite of reforms to deliver a vetting standard to enable consistency, assurance and transferability of the Government's highest-cleared workforce.

The vetting capability consolidation will deliver enhanced cooperation and efficient use of resources by intelligence agencies, and position the Government to better manage and combat the threats posed to its information, people and assets.

Rigorous oversight

ASIO must always balance the protection of Australians with the protection of their rights. I do not see these as competing priorities. To the contrary, they are *complementary* priorities.

This is why I welcome the rigorous oversight provided by the Inspector-General of Intelligence and Security—who has powers equivalent to a royal commission—and the Parliament.

This is why I am committed to ensuring our activities are always proportionate to the threat we are confronting and we are using the least intrusive methods possible.

It is why I am determined that ASIO always acts within the letter *and the spirit* of the law.

And it is why I place such emphasis on governance, accountability and transparency.

ASIO's Annual Report is an important part of my 'trust agenda', complementing my regular appearances before Senate Estimates, Parliamentary Committees and my Annual Threat Assessment.



Mike Burgess

Director-General of Security

2



A photograph of a modern office lobby with large windows and people. The image is overlaid with a teal gradient and a large number '2'.

2

OVERVIEW OF ASIO

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* (ASIO Act).

‘Security’ is defined in section 4 of the ASIO Act as the protection of Australia and its people from:

- espionage;
- sabotage;
- politically motivated violence;
- promotion of communal violence;
- attacks on Australia’s defence system; or
- acts of foreign interference;

whether directed from, or committed within, Australia or not; and

- the protection of Australia’s territorial and border integrity from serious threats.

The definition of security also extends to the carrying out of Australia’s responsibilities to any foreign country in relation to matters noted above.

ASIO achieves its purpose by obtaining, correlating, evaluating and communicating intelligence relevant to security.

Our anticipatory role means we pursue intelligence which enables the detection of adverse security events at their earliest stage.

ASIO also has a function to obtain foreign intelligence within Australia.

We protect Australia and Australians by:

- understanding our security environment and identifying security threats;
- hardening the environment against future threats; and
- working with partners to disrupt threats and reduce harm.

We communicate and advise to inform operational action, government decision-making, policy development and community resilience. We work with other agencies and authorities to achieve outcomes that protect Australia’s national interests.

The Director-General of Security is an independent statutory office holder with specific responsibilities under the ASIO Act to ensure the work of the Organisation is limited to what is necessary to discharge ASIO’s functions.

The Director-General of Security is responsible for ensuring ASIO is free from any influences or considerations not relevant to its functions, and to ensure nothing is done that might lend colour to any suggestions that ASIO seeks to further or protect the interests of any particular section of the community.

In 2021–22, ASIO pursued its purpose to protect Australia and Australians from threats to their security through five key priorities:

- counter-terrorism;
- counter-espionage and foreign interference;
- border security;
- ASIO's capability program; and
- risk and compliance.

Part 4 of this report summarises our performance in relation to these priorities during 2021–22.

Commitment to legality and propriety

ASIO operates in proportion to the threats Australia faces, within the letter and the spirit of the law, and in line with the standards and expectations of the Australian community. We are subject to a comprehensive oversight and accountability framework which underpins and supports our commitment to legality and propriety.

ASIO's accountable authority

Mr Mike Burgess, the Director-General of Security, was ASIO's accountable authority during the 2021–22 reporting period.

Mr Burgess commenced as Director-General of Security on 15 September 2019.

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

Our most important asset is our people

All of our teams contribute to our mission—protecting Australia and Australians from threats to their security. Our success is built on the imagination and intelligence of our team.

ASIO's employees are ordinary Australians who do extraordinary things. They are former nurses, trades professionals, podiatrists, teachers, engineers, geologists, athletes and journalists. They are carers, parents, grandparents and community volunteers. They pay mortgages, coach sporting teams, care for loved ones and volunteer to fight fires or patrol beaches. They are your neighbours and part of your community. The only difference is, they don't tell you where they work or what they do.

ASIO desires and requires diversity. We are proud Aboriginal and Torres Strait Islander peoples and second and third generation Australians. We are introverted, extroverted and neurodiverse. We want every ASIO officer to bring their unique skills, experience, perspectives and whole selves to work.

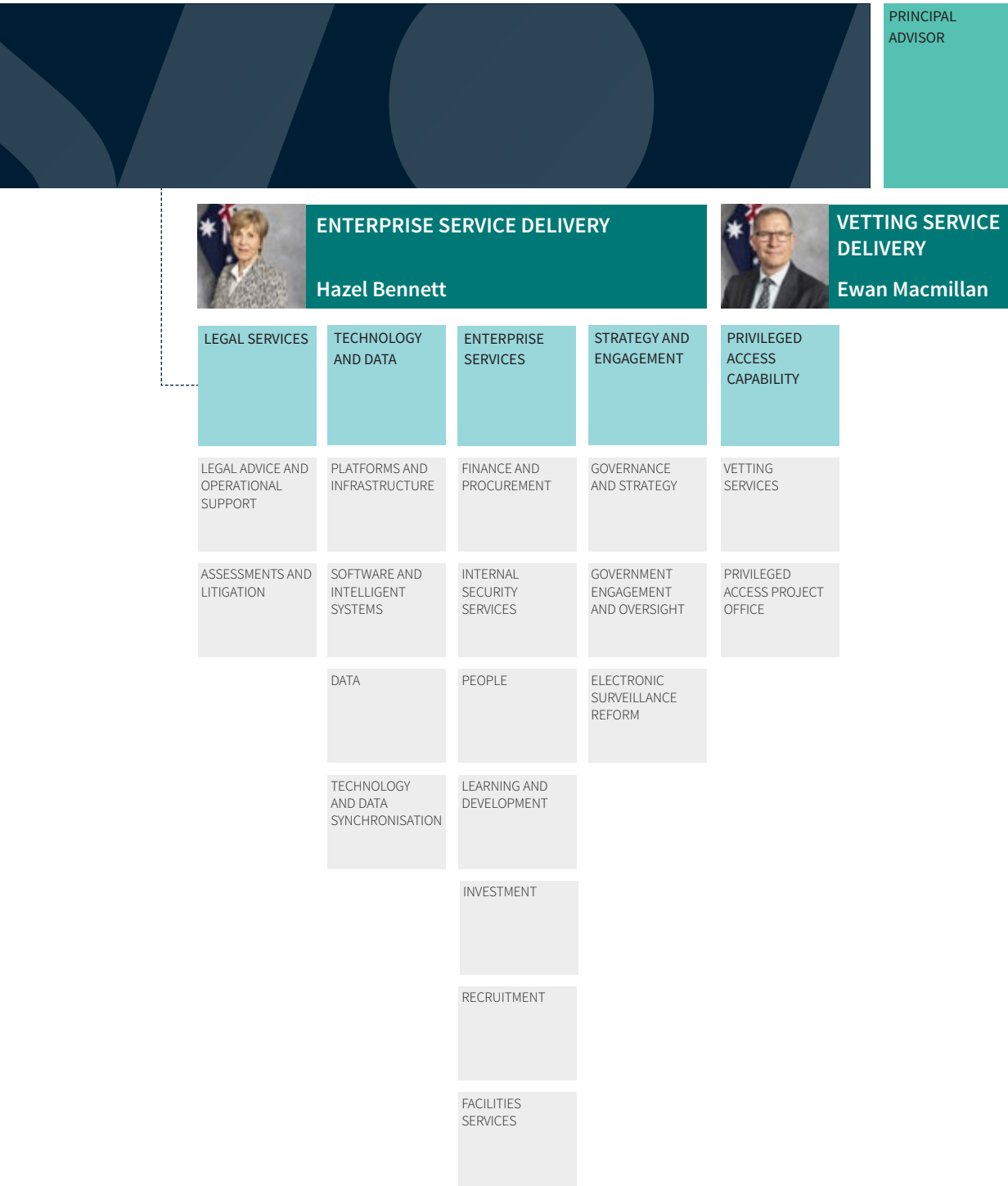
There is no ASIO type, other than innovative problem solvers—lateral, critical and creative thinkers. Our people think outside the box to get into it without being detected. They out-think, out-imagine and out-manoeuvre Australia's adversaries.

In 2021–22 we recruited 153 new staff to a diverse range of roles in technology, intelligence and corporate areas. We will continue to seek exceptional Australians for exceptional careers at ASIO.

Organisational structure



Figure 1: ASIO's organisational structure at 30 June 2022



3

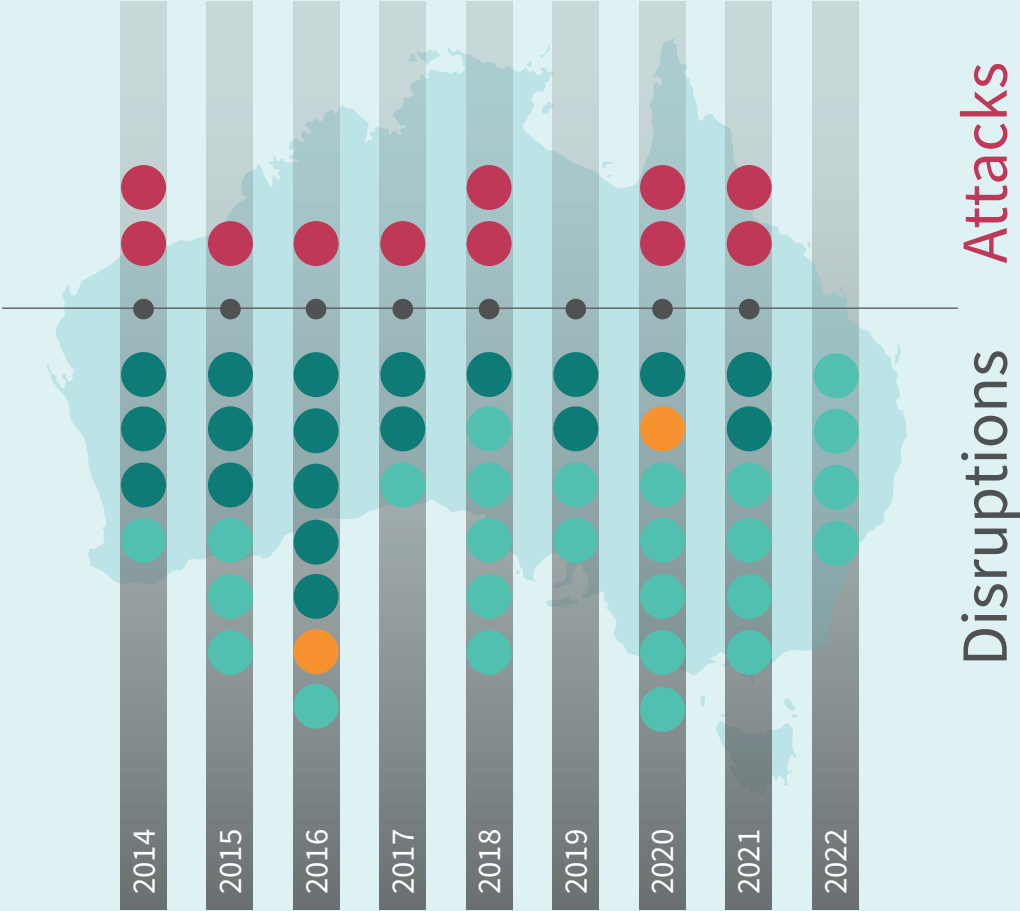






An aerial photograph of a city skyline, featuring various high-rise buildings and a prominent curved structure in the foreground. The image is overlaid with a teal gradient and several semi-transparent geometric shapes, including a large number '3' in the top right corner.

3

AUSTRALIA'S SECURITY ENVIRONMENT AND OUTLOOK

Disruptions and attacks 2014–22



-  Major counter-terrorism disruption (nationalist and racist violent extremism)
-  Major counter-terrorism disruption (Sunni violent extremism)
-  Domestic terrorist attack
-  Major espionage and foreign interference disruption

Australia's security environment and outlook

Threats to Australia's security feature both persistent elements and more dynamic ones that change relatively quickly. Some threats are fashioned by long-term forces in the global and domestic environments, while others have more direct and short-term impacts. Threats to our way of life increasingly demand that we shift our focus, with espionage and foreign interference now more prominent threats. The threat from hostile foreign powers and their proxies is pervasive, multi-faceted and has the potential to cause serious harm to our sovereignty, values and national interest. These threats originate from multiple countries—not just those that might be considered traditional adversaries.

Threats to life will always remain a priority for ASIO. Although we are seeing a reduction in the number of violent extremists who have both the intention and capability to undertake terrorist attacks in Australia, the threat remains real.

Rapidly evolving technologies and emerging issues continue to reshape the security environment. From the radicalisation of young people to COVID-19 fuelling grievances in society, and the challenge of cyber threats across our networked society and online 'safe havens' that advocate extremist ideologies, identifying threats becomes harder and requires new approaches and new expertise.

The interplay of existing challenges with new and emerging ones has changed how we might categorise them. A foreign power can simultaneously be interfering, spying and using cyber means to position for sabotage, for example.

ASIO operates within the security environment, aware of its challenges and dynamics, and we adapt our responses to best effect.

Threats to our way of life

Espionage and foreign interference have now supplanted terrorism as our principal security concern and will continue to dominate. These actions by hostile foreign powers are attacks on our way of life—they seek to undermine our liberal democratic values and systems.

Foreign interference involves clandestine, deceptive or threatening activity conducted on behalf of a foreign power which aims to affect political or governmental processes or is otherwise detrimental to Australia's interests.


Foreign interference activities are directed into many aspects of Australian society—our communities, values and freedoms, political systems, and our national industrial and research base. Foreign powers and their proxies engaging in this activity wield a range of capabilities and harbour various motivations to promote their interests covertly at the expense of Australia.

Foreign powers and their proxies remain determined to interfere in Australia's democracy and undermine our sovereignty for their own ends. However, Australia's democracy is robust and our electoral system is resilient to attempts at interference. To help protect our key institutions and ensure electoral integrity in the lead-up to the 2022 federal election, ASIO continued to support the Australian Electoral Commission.

Foreign powers and their proxies have also targeted Australia's universities and research sector to shape discourse, promote research to the foreign powers' strategic benefit, and to interfere in the lives of Australian students and staff when they have travelled overseas. To help build resilience in the sector, ASIO contributed to the refreshed guidelines released by the University Foreign Interference Taskforce.

Foreign powers and their proxies, including intelligence services, continue to seek to interfere in Australia's emerging technology endeavours, and to steal proprietary, sensitive and commercially valuable Australian information. Successful foreign intelligence operations can enable foreign governments to cut the time and cost required to replicate a desired technology, as well as to compromise Australian sovereign capability.

ASIO assessed early in the COVID-19 pandemic that foreign governments would seek to take advantage of the changed circumstances it brought on to further their own strategic ambitions. As universities and researchers conduct more of their core business online, this offers a larger potential target for hostile cyber activity.



Espionage is the theft of Australian information or capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country.

Foreign powers and their proxies continue to seek to steal information about Australia's political system, defence capabilities and operations, national security arrangements, unique science and technology capabilities, our economic and trade advantages, our diaspora communities, and databases of personal information.

Espionage enables other activities by the foreign power—for example, further acts of espionage, foreign interference, sabotage, or economic, political, or military responses.

The espionage efforts of our adversaries are directed at all levels of government as well as Australia's science and technology sectors, both military and civilian. Australia's increasing military capabilities and defence industry make us an attractive target. ASIO works with partners across government and the private sector, including in defence, to protect against these national security threats.

Cyber espionage remains the most pervasive approach adopted by our adversaries. The increasing digitisation of our economy, coupled with changes in how and where people work, will create new vulnerabilities which, when targeted, could have significant consequences for our economic prosperity, security and sovereignty. A more interconnected society—combined with evolving hostile cyber capabilities—will continue to provide foreign powers with opportunities and the means to remotely disrupt and/or damage Australia's infrastructure and economy.

ASIO also continues to see hostile powers using online and social media methods to seek to recruit Australians to give them privileged access or information. Separate to espionage funded by hostile powers, there continue to be instances that ASIO identifies of individuals abusing their privileged access to information.

Sabotage is damaging or disruptive activity against infrastructure—including electronic systems—to undermine Australia's national security or advantage a foreign power. Acts of sabotage are not limited to irreversible, destructive attacks on physical infrastructure, and can include small-scale, selective and temporary acts of degradation or disruption to networked infrastructure.

Cyber-enabled disruptive and damaging attacks on infrastructure are well within the reach of some foreign powers. These attacks have been used abroad by foreign powers as coercive or punitive means to achieve economic or geopolitical objectives against other countries.

To date we have not observed an attack of this nature in Australia, but we assess it is possible. Vulnerabilities within Australia's highly interconnected infrastructure networks provide opportunities for foreign powers to pre-position and deploy their disruptive and damaging cyber capabilities.

Attacks against infrastructure in other nations, while attributed to criminal groups, demonstrate the potential harm that may result from cyber-enabled disruptive and damaging activities.

Threats to life

Overall, we are seeing a reduction in the number of violent extremists who have both the intention and capability to undertake terrorist attacks in Australia. This is down from a peak during the height of the Islamic State of Iraq and the Levant's (ISIL) global terrorism campaign. The threat is not extinguished though, and extremists across the ideological spectrum remain committed to their belief in the legitimacy of violence to achieve their political ambitions.

Sunni violent extremism represents an enduring threat. Religiously motivated violent extremist groups such as ISIL and their affiliated groups, and al-Qa'ida, continue to justify violence against the West, including Australia.

Driven by local agendas—but with global ambitions—these groups thrive, either physically or virtually, in unstable regions of the Middle East, Africa and South Asia, promulgating their ideology, undertaking attacks and encouraging their adherents to engage in violence. Their messaging continues to be consumed by violent extremists globally, including Sunni violent extremists here in Australia, across a variety of online platforms.

In South-East Asia, violent extremists under ISIL's influence are adapting their methods. In Indonesia, Jemaah Islamiyah continues to recruit, train and prepare for possible future violence. Cross-border links across the region, and beyond to international conflict zones, increases the risk of uptake of new skills and know-how, attack methods and ideology, altering the threat environment in South-East Asia.

Challenges to the environment in South-East Asia include the scheduled release of convicted terrorists and the return of individuals from Syria and Iraq. Many of these terrorist detainees probably maintain their violent extremist ideologies and the release of some will reintroduce terrorist capability into the environment.

The global growth in ideologically motivated violent extremism, particularly nationalist or racially motivated violent extremists, has been reflected in Australia. This has changed what was once a largely, but not solely, single prominent hue of concern related to religiously motivated violent extremism into a rainbow of ideologies and justification for violence in support of them (see Text box 1).

Specific and single-issue violent extremists of various ideological strains and influences persist. The COVID-19 lockdowns provided more opportunity for isolated Australians to be exposed to online extremist or conspiracy theory messaging and misinformation. Some of these theories and worldviews justify violence and have led to specific-issue violent extremism in Australia. Over the last year we have seen an increase in the willingness of a minority of protesters to adopt violence as a tactic including attacking police, damaging property, or inciting others to do so.

Text box 1: nationalist and racist violent extremism

ASIO continues to see Australians drawn to nationalist and racist violent extremist ideologies.

A key belief system in this cohort is the belief in an 'inevitable race war'. There is a broad acceptance that at some stage in the future, society will collapse and a conflict will break out along racial or ethnic lines, after which there will be the creation of a white ethno-state.

The vast majority believe that because this race war is 'inevitable', the most important thing right now is to prepare for the impending war. This 'prepping' behaviour includes stockpiling firearms and ammunition, learning survivalist skills, and seeking to be self-sufficient.

For others, they do not want to wait for the war, and instead try to 'accelerate' the process of the race war starting—we call people who subscribe to this belief-set 'accelerationists'.

The behaviour of some groups and associated nationalist and racist violent extremists is becoming more overt and provocative. In some cases, leading to violent confrontations with members of the public.



While there has been a reduction in the number of extremists with the intent to undertake a terrorist attack, we have seen an increase in the number of minors represented in ASIO investigations. We see this worrying trend in both the religiously and ideologically motivated violent extremism spaces. Addressing this trend requires a whole-of-government and community approach, with the radicalisation of minors occurring due to a variety of sociological, ideological and personal reasons.

Both religiously and ideologically motivated violent extremist groups have produced sophisticated online propaganda which calls on lone actors

to engage in violence, and provides technical advice to do so (see Text box 2). And our greatest concern continues to be the threat of a terrorist attack undertaken by a single individual or a small group—irrespective of their specific ideology. Such attacks are difficult to detect and can occur with little to no warning.

A terrorist attack in Australia is more likely to involve readily acquired weapons—such as knives and vehicles, explosives and/or firearms—and relatively simple tactics. We have seen increased interest in new technologies, including 3D printed firearms and more complex attack methodologies.

Text box 2: the online environment

The internet—primarily via social media and encrypted communication applications—enables the dissemination and discussion of violent extremist material within secure, online echo chambers. The high levels of violent rhetoric within some of these online extremist networks is concerning and, while violent rhetoric does not generally translate to actual violence, the normalisation and legitimisation of violent responses to public policy probably increases the likelihood an individual somewhere will mobilise to violence.



We have seen extremist ideologues, in Australia and offshore, seeking to incite this violence within the community and against the government by combining conspiracy theories with highly emotive propaganda, particularly in relation to COVID-19. COVID-19 disinformation, sown by some foreign powers and their proxies, has also been consumed and amplified within these online echo chambers—both knowingly and unwittingly. These foreign powers view such networks as potential vectors to undermine Australian security by generating uncertainty, division and unrest within the community.

4



4

REPORT ON PERFORMANCE



Annual performance statement 2021–22

Introductory statement

I, as the Director-General of Security and the accountable authority of ASIO, present the 2021–22 annual performance statement for ASIO, as required under paragraphs 39(1)(a) and (b) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

In my opinion, this statement accurately presents the performance of ASIO in achieving its purpose and complies 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

Summary of results

Key performance measures—2021–22		Target (2021–22)	Outcome
Measure 1	Counter-terrorism: impact of operational activities advice	80%; HIGH	ACHIEVED
Measure 2	Counter-terrorism: impact of policy development advice	80%; HIGH	PARTIALLY ACHIEVED
Measure 3	Counter-espionage and foreign interference: impact of operational activities advice	80%; MEDIUM	ACHIEVED
Measure 4	Counter-espionage and foreign interference: impact of policy development advice	80%; MEDIUM	ACHIEVED
Measure 5	Border security: impact of operational activities advice	70%; MEDIUM	ACHIEVED
Measure 6	Border security: impact of policy development advice	70%; MEDIUM	ACHIEVED
Measure 7	ASIO capability program: ASIO capability delivery	Delivery of capability milestones	ACHIEVED
Measure 8	Risk and compliance: risk management framework	Adherence to Commonwealth Risk Management Policy requirements	ACHIEVED

Summary of results

The security environment remained complex, challenging and changing in 2021–22. ASIO delivered significant outcomes in the 2021–22 year and met seven of its eight performance measures, partially achieving the remaining measure.

ASIO has continued to protect Australia and Australians from terrorist threats in 2021–22. We achieved this through intelligence collection, investigation and analysis, and by providing our stakeholders assessments and advice. We have worked to understand the terrorist threats we face, harden the environment against those threats, assist partners to disrupt terrorist attacks, and support law enforcement arrests and convictions. During 2021–22 we saw the terrorist threat further diversify. The online environment is amplifying a range of grievances and the trend of increased radicalisation among young Australians has continued. ASIO remains well positioned to address future challenges in the terrorism environment. Our well-established relationships and contribution to Australia's counter-terrorism frameworks will enable our continued success.

In 2021–22, espionage and foreign interference supplanted terrorism as ASIO's principal security concern. Threats of foreign interference and espionage are pervasive and enduring, with espionage and foreign interference in Australia continuing at an unacceptably high level. In this challenging environment, ASIO has excelled against the ambitious targets we set for ourselves in 2021–22.

Our counter-espionage and foreign interference frameworks have matured, including Counter Foreign Interference Taskforce arrangements, which position ASIO well to counter this threat. During 2021–22, we continued to provide trusted advice to Government and industry on the espionage and foreign interference threat. We protected Australia by identifying and understanding the nature of these threats, establishing a less permissive environment for foreign actors to undertake this activity, and worked with partners to reduce harm.

In 2021–22, ASIO continued to support policy development and operational engagement related to Australia's border integrity. This was achieved in the context of a changed border security threat environment as a result of COVID-19. We supported Australia's border integrity by providing analysis and security advice in relation to people smuggling activities, complex visa applications, and other movements of goods and people.

ASIO's performance against our counter-terrorism, counter-espionage and foreign interference and border security performance measures was bolstered by our focus on accelerating our capability development and maintaining a robust risk and compliance framework. We saw considerable improvement in the impact of policy development advice in counter-terrorism, partially achieving our ambitious target on this performance measure. Delivery against our capability program and risk and compliance performance measures has positioned ASIO to meet future challenges, stay ahead of technological change, and accept and engage with risk.

Reporting framework

ASIO operates under the Australian Government's outcomes and programs framework. Outcomes are the intended results, impacts or consequences of actions by the government as defined in the portfolio budget statements for Commonwealth entities. Government programs are the primary vehicle by which entities achieve their intended purposes.

Performance reporting requirements are part of the Commonwealth performance framework established by the *Public Governance, Performance and Accountability Act 2013*.

It is anticipated this performance statement will be read with broader information provided in the *ASIO Corporate Plan 2021–25* and the Home Affairs Portfolio Budget Statements (PBS), to provide a complete picture of ASIO's planned and actual performance.

The alignment between ASIO's purpose, as set out in the *ASIO Corporate Plan 2021–25* and the Outcome and Program in the ASIO Budget Statement 2021–22 is shown below.



ASIO's purpose

ASIO protects Australia and Australians from threats to their security. Our purpose is defined in the *ASIO Corporate Plan 2021–25*.

In 2021–22 ASIO achieved this purpose by delivering outcomes against each of the Organisation's key priorities, outlined below.

Counter-terrorism

ASIO has countered terrorism by protecting Australians from religiously motivated and ideologically motivated violent extremism. The Organisation has continued to collect intelligence within Australia and overseas, analyse and investigate terrorist threats, and work with partners to strengthen public safety and intervene to disrupt attacks. Our intelligence collection, investigation and assessment efforts have enabled ASIO to identify and understand the threats we face, and to provide impactful advice that hardened the environment against, and informed government policy and responses to, violent extremism.

Counter-espionage and foreign interference

ASIO has countered espionage and foreign interference by protecting Australia from threats posed by foreign intelligence services seeking to undermine Australia's democratic systems and institutions. ASIO has collected intelligence on, and investigated, threats targeting Australian interests. The Organisation has continued to provide impactful and trusted advice to government and industry, and worked to disrupt and deter those attempting to undermine our national interests through espionage and foreign interference. We have identified and worked to understand the threats we face, established a less permissive environment for espionage and foreign interference, and worked to reduce harm.

Border security

ASIO has continued to support whole-of-government efforts to protect Australia's border integrity. The Organisation has provided analysis of, and security advice on, people smuggling activities, complex visa applications, and other movements of goods and people. This has assisted our partners to maintain the integrity of Australia's border protection programs.

Capability program

ASIO is committed to accelerating our ability to achieve our purpose, deliver against our priorities and position the Organisation to meet future challenges. Through a human-led, data-driven, technology-enabled approach, our capability program aims to address capability gaps, keep ASIO in step with technological change, and maintain our ability to detect the early signs of threat activity. The program supports our ability to invest in, and sustainably adopt, new technology and tradecraft practices. This includes partnering with the Australian technology sector in the development of sovereign capabilities in key areas of national security, and further cementing our contribution to, and ongoing benefit from, our strategic partnerships. Improved application of commercial technologies enables a more agile and sustainable response to changes in the rapidly evolving technology environment.

Risk and compliance

Accepting and engaging with risk is inherent to our role of protecting Australia and Australians from threats to their security. In a complex security environment, our risk and compliance frameworks enabled informed decision-making and effective prioritisation. ASIO officers continued to act with integrity. We have been impartial, committed to our purpose, and operated ethically and with propriety. Our frameworks supported our compliance with the law and enabled dynamic responses to our evolving threat environment.

Performance measures

This annual performance statement provides an assessment of ASIO’s achievement of the performance measures set out in the *ASIO Corporate Plan 2021–25*.

The measures relating to counter-terrorism, counter-espionage and foreign interference, and border security (measures 1–6) focus on the level of impact of ASIO operational and/or policy advice. When assessing impact, we consider whether:

- ASIO advice provided context;
- ASIO advice was relevant and practical; and
- ASIO advice influenced stakeholder decision-making.

For the purposes of this report, ‘advice’ encompasses all forms of communication to the Australian Government, government agencies, and industry and community sector stakeholders that conveys ASIO’s expertise, intelligence, assessments, priorities and recommendations on security matters.

The following definitions were shared with key stakeholders when determining what level of impact our advice (policy and/or operational) has had on their decision-making.

LOW	MEDIUM	HIGH
Our advice provided little or no context, and did not influence your decision-making.	Our advice provided context; was relevant and practical; and, influenced your decision-making.	Our advice was timely and relevant; practical, focused and provided or enabled exercisable options; and directly informed and shaped your decision-making.

The measures relating to ASIO’s capability program and risk and compliance priorities (measures 7–8) focused on the delivery of mission effects and outcomes through the delivery of capability program objectives and milestones, and adherence to the requirements of the Commonwealth Risk Management Policy.

Further details, rationale and targets related to all ASIO performance measures are discussed in the *ASIO Corporate Plan 2021–25*.

Performance methodology

Performance against ASIO's priorities has been measured through a combination of quantitative and qualitative methods, including defined targets, case studies, stakeholder feedback and identified milestones. Our performance—and the delivery of impactful effects and outcomes against these priorities—is measured and reported in a manner which safeguards our sensitive capabilities, information and tradecraft.

This annual performance statement is the second year we have assessed our performance using percentage-based impact targets (measures 1–6). Measuring outcomes in this way is important to ensure we are focusing our efforts and delivering meaningful advice to stakeholders. We will continue to progressively refine our performance measures to improve our ability to measure ASIO's impact and demonstrate our effectiveness in a transparent way.

Assessment of our performance against measures relating to counter-terrorism, counter-espionage and foreign interference, and border security (measures 1–6) has been informed by stakeholder feedback throughout the year, including ASIO's annual survey of key stakeholders, undertaken by an independent surveyor.

Stakeholders are:

- drawn from relevant federal, state and territory governments, and private enterprise;
- ongoing, frequent recipients of ASIO advice; and
- engaged in operational activities or policy development related to ASIO's key activities.

The 2022 ASIO stakeholder survey collected quantitative and qualitative data on ASIO's performance from 68 stakeholders from a wide cross-section of commonwealth and state departments and agencies, and from industry and academia. Feedback was sought against performance measures 1–6 as well as more generally in relation to ASIO's value, engagement and impact.

The 2022 survey used a combination of written questionnaires (48 stakeholders) and interviews (36 stakeholders) to seek stakeholder's views—16 stakeholders completed both a questionnaire and interview.

Survey results were used to determine ASIO's performance against measures 1–6. Further context on our performance was gathered through internal triannual performance reporting and regular stakeholder engagement throughout the year. Similarities in measures 1–6 between the 2020–21 and 2021–22 reporting periods have also allowed for a comparison of our results over time. These trends are discussed as part of our 2021–22 performance report.

Assessment of our performance against our capability program measure (measure 7—ASIO capability delivery) has been informed by a range of inputs, including independent review, internal and external program governance, assessments of benefits realisation, staff feedback, the development of key enabling partnerships, the on-boarding of capability-related resources, and other program delivery metrics such as budget and time frame.

Our performance against our risk and compliance measure (measure 8—risk management framework) has been informed by an assessment of our compliance with the Commonwealth Risk Management Policy, which sets out nine elements with which entities must comply in order to establish an appropriate system of risk oversight and management.

Qualitative and quantitative methodologies

P E R F O R M A N C E M E A S U R E S		Defined targets	Case studies	External surveys/ assessments	Stakeholder feedback	Identified milestones
	1	Counter-terrorism: impact of operational activities advice				
		✓	✓	✓	✓	
	2	Counter-terrorism: impact of policy development advice				
		✓	✓	✓	✓	
	3	Counter-espionage and foreign interference: impact of operational activities advice				
		✓	✓	✓	✓	
	4	Counter-espionage and foreign interference: impact of policy development advice				
		✓	✓	✓	✓	
	5	Border security: impact of operational activities advice				
		✓	✓	✓	✓	
	6	Border security: impact of policy development advice				
		✓	✓	✓	✓	
	7	ASIO capability program: ASIO capability delivery				
		✓		✓	✓	✓
	8	Risk and compliance: risk management framework				
		✓				✓

Analysis of performance

ASIO achieved its purpose during the 2021–22 reporting period through the delivery of outcomes against our key priorities.

ASIO's stakeholders were overwhelmingly positive about ASIO's impact in 2021–22. The 2022 independent stakeholder survey reported that ASIO is highly rated on its professionalism, subject matter expertise, and responsiveness. The ASIO of 2022 is seen as a more engaged and open Organisation which is more attuned to the interests, needs and equities of its stakeholders.

Stakeholders commented that ASIO's higher public profile has strengthened its reputation and impact. Greater engagement in the public sphere has aided awareness of security threats and prompted important discussions on security issues within departments and agencies, as well as with industry and international partners.

Partners commented favourably on ASIO's support to their own capability development, both in terms of ASIO's advice on emerging trends in the security environment, informing capability decisions, as well as ASIO's advice into capability decisions and direct sharing of capability. This capability sharing extends across both technical and human domains—ASIO secondees embedded with partner agencies are highly valued for their subject matter expertise, understanding of the stakeholder's business needs, and networks.

ASIO's 2021–22 performance reporting saw increased impact ratings from stakeholders and an overall improvement with the achievement of seven of eight performance measures in 2021–22 compared with seven of nine measures achieved in 2020–21.

As noted in 'performance methodology', similarities in measures 1–6 between the 2020–21 and 2021–22 reporting periods have also allowed for a comparison of our results over time. Results against our counter-terrorism measures, in particular, show improvements in our impact ratings. Similarly, stakeholder ratings of ASIO's impact for countering espionage and foreign interference has increased.

We have set ambitious targets for our counter-espionage and foreign interference measures (80% HIGH) in the *ASIO Corporate Plan 2022–26*, and our 2021–22 trajectory sets ASIO up well to achieve these results.

In 2021–22, ASIO continued to protect Australia and Australians from threats to their security. We countered terrorism through intelligence collection, investigation and analysis, and provided partners with trusted advice and assessments. ASIO conducted successful operational activity to counter threats, and contributed to the operational activity of others.

We countered espionage and foreign interference from foreign powers and their proxies. We uncovered and identified threats to Australian Government, defence, political and other national interests. Our advice to government and industry raised awareness of threats and established a less permissive environment for covert actors to operate.

The scale and sophistication of the threats facing Australia required ASIO to be proactive in our advice to government and industry. ASIO continued to invest in our people and capabilities to help our stakeholders better understand, identify and manage security threats. Our continued investment in partnerships recognises that security is a shared responsibility, and ASIO will continue to work with others, across policy, law enforcement, intelligence, industry and community sectors to continue to protect Australia and Australians from threats to their security.



Counter-terrorism

ASIO has countered terrorism by protecting Australians from religiously motivated and ideologically motivated violent extremism. The Organisation has continued to collect intelligence within Australia and overseas, analyse and investigate terrorist threats, and work with partners to strengthen public safety and intervene to disrupt attacks. Our intelligence collection, investigation and assessment efforts have enabled ASIO to identify and understand the threats we face, and to provide impactful advice that hardened the environment against, and informed government policy and responses to, violent extremism.



Counter-terrorism

Result—impact of ASIO’s counter-terrorism operational activities advice

1. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a HIGH impact on their decision-making in informing counter-terrorism operational activities, managing security risks and disrupting activities that threatened Australia’s security.		
Target (2021–22)	80%; HIGH	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.14) PBS 2021–22, Outcome 1 (table 2.1.2)		
2021–2022 result		2020–2021 result	
84% HIGH; 16% MEDIUM		58% HIGH; 93% MEDIUM or higher (target: 80% HIGH)	

Stakeholder survey results against our ‘counter-terrorism—impact of operational activities advice’ were overwhelmingly positive, exceeding the target we set ourselves in the *ASIO Corporate Plan 2021–25*.

84 per cent of principal stakeholders said ASIO achieved a **HIGH** impact, with a further 16 per cent of principal stakeholders rating ASIO’s performance as **MEDIUM**.

Principal stakeholders are Commonwealth and State law enforcement agencies, national intelligence agencies, and central policy departments (Home Affairs, Prime Minister and Cabinet, Department of Foreign Affairs and Trade, Defence, Attorney-General’s and State Premiers Departments).

These stakeholders are considered by the independent surveyor to be central to the counter-terrorism mission.

This outcome represents an improvement from our results in 2020–21, when 58 per cent of respondents reported ASIO’s impact was **HIGH** (and 93 per cent of respondents reported ASIO’s impact was **MEDIUM** or higher).

Commentary and feedback provided during the survey was positive. Stakeholders noted that ASIO is a ‘professional, expert and responsive’ organisation and a ‘respected, authoritative source of threat advice and assistance’.

Stakeholder feedback shows ASIO's advice has supported an increased understanding of the terrorism environment, particularly in shaping partners' operational activity and capability investment. Partners commented on ASIO's crucial role in providing the necessary capability uplift to enable their responses to changes in the terrorism threat environment.

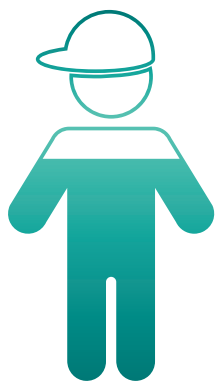
Additional feedback received throughout the year demonstrated the positive impact ASIO had on stakeholders' operational decision-making. Key themes included ASIO's advice to inform Government's High Risk Terrorism Offenders (HRTO) framework, public awareness in relation to the radicalisation of minors, and support to partners in relation to the ongoing implications of the conflict in Syria and Iraq.

Examples demonstrating ASIO's impact on counter-terrorism operational activities advice include the following.

ASIO's advice provided context, was relevant and practical, and influenced decision-making

- ASIO advice continued to inform development and implementation of the whole-of-government framework for responding to HRTOs. ASIO advice directly informed development of the HRTO Regime Implementation Framework. The framework will ensure effective coordination and interoperability between ASIO, our law enforcement colleagues, and other Commonwealth and State/Territory agencies, in managing the release of a large cohort of terrorist offenders over the next 10 years and beyond.
- In early to mid-2022, in unrelated cases, two individuals were found guilty of the offence of advocating terrorism (in contravention of section 80.2C of the *Criminal Code Act 1995*) in support of nationalist and racist violent extremist (NRVE) ideologies. Both cases commenced as ASIO investigations in 2020 and quickly transitioned to Joint Counter Terrorism Team-led criminal investigations. The offenders in these cases represent the second and third individuals convicted in Australia of terrorism-related offences because of their NRVE ideologies, and the second and third individuals convicted of the relatively new offence of advocating terrorism.
- During the reporting period, ASIO provided tailored and timely briefings to government and industry partners in relation to a range of trends and developments in the terrorism threat environment, informing partners' planning and operations.
- State partners directly attributed an increase in reporting in relation to the radicalisation of minors to increased awareness of the issue as a result of ASIO public commentary.

- ASIO provided partners with relevant and practical advice on the difference between NRVE and religiously motivated violent extremism (RMVE), in particular Sunni violent extremism, within Australia. Our advice on how the respective cohorts' source and distribute propaganda—and their comparative approaches to operational and communications security—is informing investigative strategies, operational activities, capability development and policy responses.
- During the reporting period, ASIO advice informed the operations of a range of key partners in relation to the security environment in Syria and the status of Australian women and children in Syrian internally displaced person (IDP) camps.



50%

Between July and December 2021, minors, on average, comprised more than half of ASIO's 10 highest priority counter-terrorism investigations each week

Result—impact of ASIO’s counter-terrorism policy development advice

2. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a HIGH impact on their decision-making in relation to policy development and responses to terrorism.		
Target (2021–22)	80%; HIGH	Outcome	PARTIALLY ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.15) PBS 2021–22, Outcome 1 (table 2.1.2)		
2021–2022 result		2020–2021 result	
71% HIGH; 29% MEDIUM		56% HIGH; 100% MEDIUM or higher (target: 80% HIGH)	

The 2022 stakeholder survey results against our ‘counter-terrorism—impact of policy development advice’ did not meet the ambitious targets we set ourselves in the *ASIO Corporate Plan 2021–25*.

71 per cent of principal stakeholders responded that ASIO achieved a **HIGH** impact for counter-terrorism policy development advice, with a further 29 per cent of stakeholders indicating ASIO’s advice had a **MEDIUM** impact.

Principal stakeholders are Commonwealth and State law enforcement agencies, national intelligence agencies, and central policy departments (Home Affairs, Prime Minister and Cabinet, Department of Foreign Affairs and Trade, Defence, Attorney-General’s and State Premiers Departments). These stakeholders are considered by the independent surveyor to be central to the counter-terrorism mission.

While not achieving the target of 80 per cent **HIGH** impact, these results demonstrate a considerable improvement on ASIO’s 2020–21 results. In 2020–21, 56 per cent of respondents reported ASIO had achieved a **HIGH** impact against this measure, and 100 per cent of stakeholders reported ASIO’s impact was **MEDIUM** or higher.

In particular, stakeholders highlighted the importance of ASIO’s advice in relation to the ongoing implications of foreign fighters and the Syria conflict. These stakeholders said ASIO’s work had been foundational for their consideration of residual risk and mitigation strategies. Examples used included ASIO’s contribution to whole-of-government efforts in relation to High Risk Terrorism Offenders (HRTTO) and ASIO’s advice in relation to the diversifying terrorism threat environment.

Additional feedback received throughout the 2021–22 year was similarly positive. Particular examples demonstrated ASIO's impact on listings of terrorist organisations under the Criminal Code and advice provided to government and industry to support their ability to strengthen their own security posture and reduce their exposure to terrorist threats.

Examples demonstrating ASIO's impact on counter-terrorism policy development advice include the following.

ASIO's advice provided context, was relevant and practical, and influenced decision-making

- During 2021–22, ASIO advice contributed to the development of new terrorism-related legislation and informed reviews of existing legislation to ensure they remain necessary and proportionate to the evolving terrorist threat. ASIO contributions over the period informed ongoing development of the Extended Supervision Orders (ESO) Bill and an inquiry into the operation of the Temporary Exclusion Orders (TEO) legislation.
- ASIO provided stakeholders impactful advice, intelligence assessments and briefs regarding the rise of ideologically motivated violent extremism (IMVE) actors and groups in Australia and their security relevance.
- During 2021–22, ASIO attended the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the re-listing of Hamas's Izz al-Din al-Qassam Brigades, as part of its review into the re-listing of five terrorist organisations.

ASIO advice informed the Committee's recommendation to expand the listing to the entirety of Hamas, which was accepted by the Government.

- ASIO's timely, relevant and practical advice on proscription cases during the reporting period empowered whole-of-government decision-making on terrorist organisation listings to harden the environment and enable activities to disrupt the capabilities of terrorist organisations. ASIO advice contributed to the listing of 15 terrorist organisations under the Criminal Code during 2021–22.
- During the 2021–22 period, ASIO threat assessments and analytical reports provided context to government, foreign intelligence and security partners, and industry stakeholders on specific security environments, global terrorism trends and developments, and key threat actors and targets.
 - Targeted advice was provided to more than 40 representatives from the Australia-Africa Minerals & Energy Group to enhance the security of Australians and Australia's interests against terrorist threats in the region. Partnering with the Department of Foreign Affairs and Trade (DFAT), ASIO addressed ongoing concerns of Australian companies related to their employees' safety due to the rising number of terrorist attacks in regions where Australian mining sites are located.

- ASIO's biannual threat assessment was shared with business and industry subscribers via the ASIO Outreach Portal and in external engagements. Our advice highlighted the increasing volatility in the security environment driven by specific-issue grievances surrounding the pandemic.
- ASIO advice supported government and businesses to strengthen their security posture and reduce exposure to threats.
- An OFFICIAL version of ASIO's annual Crowded Places Threat Assessment has had wide reach and impact with government and industry. It has been viewed/downloaded hundreds of times since being added to the Outreach portal in November 2021.
- During the reporting period, our advice and intelligence informed whole-of-government efforts to mitigate the terrorist threat to Australians and Australian interests, including through:

144 544

ACCESS SECURITY ASSESSMENTS

131 877

to AusCheck, including for individuals seeking Aviation Security Identification Cards (ASICs) and Maritime Security Identification Cards (MSICs)



12 667

individuals seeking access to security-sensitive chemicals, biological agents or nuclear sites



479

Counter-terrorism products



88

Products that span both counter-terrorism and counter-espionage and foreign interference



Counter-espionage and foreign interference

ASIO has countered espionage and foreign interference by protecting Australia from threats posed by foreign intelligence services seeking to undermine Australia's democratic systems and institutions. ASIO has collected intelligence on, and investigated, threats targeting Australian interests. The Organisation has continued to provide impactful and trusted advice to government and industry, and worked to disrupt and deter those attempting to undermine our national interests through espionage and foreign interference. We have identified and worked to understand the threats we face, established a less permissive environment for espionage and foreign interference, and worked to reduce harm.

Counter-espionage and foreign interference

Result—impact of ASIO’s counter-espionage and foreign interference operational activities advice

3. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our counter-espionage and foreign interference advice had a MEDIUM impact on their decision-making in informing counter-espionage and foreign interference operational activities, managing security risks and disrupting activities that threatened Australia’s security.		
Target (2021–22)	80%; MEDIUM	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.16) PBS 2021–22, Outcome 1 (table 2.1.2)		
2021–2022 result		2020–2021 result	
80% HIGH; 12% MEDIUM		89% MEDIUM or higher (target: 70% MEDIUM)	

The 2022 stakeholder survey results show ASIO exceeded targets against our ‘counter-espionage and foreign interference—impact of operational activities advice’ measure set in the *ASIO Corporate Plan 2021–25*.

In 2022, 80 per cent of stakeholders rated ASIO’s impact on counter-espionage and foreign interference operational activity as **HIGH**. A further 12 per cent rated ASIO’s impact as **MEDIUM**. These results demonstrate a significant improvement on our 2020–21 results, when 89 per cent of stakeholders rated our support as **MEDIUM** or higher.

These results were also delivered in an environment where espionage and foreign interference overtook terrorism as ASIO's principal security concern, reflecting the increasing prominence of our efforts against this threat.

In particular, stakeholders noted the importance of ASIO's public statements and outreach. The ASIO of 2022 is seen as an engaged and open partner that is more attuned to the equities of others. The work of ASIO's outreach and engagement across government, industry and other sectors was highlighted. Feedback demonstrated ASIO's impact on partners' understanding of the threat environment, enabling those partners to more proactively harden their organisations against threats. Greater information sharing, particularly in relation to the ASIO-led Counter Foreign Interference Taskforce (CFITF) was also highlighted.

Similar feedback was provided by stakeholders throughout the year, including on the support ASIO provided to inform their own hardening against compromise, ASIO's support to electoral integrity processes, and our advice to Defence in relation to the security implications of AUKUS.

Further examples demonstrating ASIO's impact on counter-espionage and foreign interference operational activities advice include the following.

ASIO's advice provided context, was relevant and practical, and influenced decision-making

- During the reporting period ASIO investigations identified multiple compromises of Australian victims by state-sponsored cyber groups and worked with victims and the Australian Cyber Security Centre (ACSC) to protect the sensitive information contained in these systems.
- During 2021–22, ASIO published advice on the full spectrum of threats faced by Australia's data storage and processing sector. This suite of assessments, which included unclassified material provided to industry partners, continues ASIO's broader strategy of supporting sectors to harden against foreign interference.
- We contributed to an education and hardening campaign targeting the Australian clearance holder cohort, covering responsibilities, obligations and contact reporting requirements. This campaign across government and industry is designed to bring about positive changes in clearance holder behaviour.
- ASIO advice shaped stakeholder improvements to protection mechanisms for Australian intellectual property with dual-use or military applications.
- ASIO's bilateral secondment arrangements with the Australian Government Security Vetting Agency continue to contribute to collaboration and provide context to decision-making, processes and requirements for both organisations.

- ASIO protected government information from compromise during the reporting period by assisting with the identification of potential malicious insiders, promoting stronger security cultures and lifting federal agency contact reporting rates. Our advice significantly improved security posture across multiple government agencies.
- ASIO broadened efforts to increase government and industry partner understanding of, and resilience to, espionage, foreign interference (EFI) and sabotage threats to critical infrastructure sectors, through the sharing of assessments and advice and our active outreach program. During the period we published OFFICIAL level ASIO assessments on EFI threats to the mining and resources, data storage and processing, banking and finance, and healthcare and medical sectors. We provided briefings to or engaged with partners in the aviation, financial, mining, quantum research, energy and maritime sectors.
- ASIO provided advice and oversight in the trial for a new access check scheme, the Naval Shipbuilding Sustainment Identity Card (NSSIC). The scheme was trialled as a mechanism to identify individuals of security concern at the Osborne Naval Ship facility. The NSSIC scheme will be rolled out formally for the Osborne precinct in early 2023 and we anticipate receiving around 7500 checks over the next 12 months.
- During the reporting period, ASIO hosted the inaugural annual CFITF conference with State and Federal police counterparts. The conference was focused on increasing understanding of the CFITF construct and delivering thematic briefs with a focus on community interference. We shared advice on integration of State police into CFITF activities and community interference responses which will help in hardening the environment at a local level.
- Throughout 2021–22, ASIO continued a focus on education campaigns for clearance holders and engagement with government agencies to harden against foreign intelligence service access to government information through the insider threat. ASIO presented at a range of fora including agency induction courses, insider threat seminars and security awareness courses for government officials posted overseas.



NITRO REPORT PRYING MINDS

CASE STUDY



In early 2022, ASIO launched the Prying Minds campaign to provide defence industry with information on the threat from foreign intelligence activity. As part of the campaign, an online portal—**Notifiable Incidents, Threats and Reportable Observations (NITRO)**—was established, to provide a mechanism for non-clearance holders to report information related to espionage, insider threats or foreign interference. The portal and campaign are specifically designed to provide a mechanism to collaborate with business and institutions to help preserve Australia's sovereign capability and commercial and scientific advantage and protect Australia's \$270 billion investment in defence industry.

We estimate the reach of the message to our target audience via launch activities (a dedicated webpage hosting a suite of information resources and an extensive outreach program including social media), was tens of thousands. In addition, ASIO continues to support the hardening of 15 000 small and medium defence industry companies against espionage and foreign interference, via targeted engagements and threat briefings Australia-wide.

Result—impact of ASIO’s counter-espionage and foreign interference policy development advice

4. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our counter-espionage and foreign interference advice had a MEDIUM impact on their decision-making in relation to espionage and foreign interference-related policy development and responses to this threat.		
Target (2021–22)	80%; MEDIUM	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.17) PBS 2021–22, Outcome 1 (table 2.1.2)		
2021–2022 result		2020–2021 result	
73% HIGH; 24% MEDIUM		100% MEDIUM or higher (target: 70% MEDIUM)	

Like measure 3, 2022 stakeholder survey results show ASIO well exceeded the targets set against our ‘counter-espionage and foreign interference—impact of policy development advice’ measure set in the *ASIO Corporate Plan 2021–25*.

73 per cent of stakeholders reported that ASIO had a **HIGH** impact on their decision-making. A further 24 per cent rated ASIO’s impact as **MEDIUM**. These results were an improvement on ASIO’s 2020–21 results, demonstrating the increasing prominence of espionage and foreign interference threats and demand for ASIO reporting, assessments and advice.

ASIO’s public profile was again highlighted as a positive factor in strengthening ASIO’s reputation and impact, and in helping to raise awareness of security threats. ASIO is seen to be more open with trusted partners, and more attuned to the interests of policy agencies. Survey respondents noted the importance of ASIO building community understanding of threats.

Feedback received from stakeholders throughout the year noted ASIO’s increased efforts to produce assessments and advice for a broader audience, and the support and advice provided to harden Australia’s electoral institutions.

Further examples demonstrating ASIO's impact on counter-espionage and foreign interference policy development advice include the following.

ASIO's advice provided context, was relevant and practical, and influenced decision-making

- In 2022, ASIO contributed advice to support whole-of-government responses to Russia's invasion of Ukraine.
- Throughout 2021–22, ASIO worked to produce an increased number of assessments at the OFFICIAL classification level to provide context and reach a broader cross-section of stakeholders. This relevant and practical advice generated significant interest from ASIO's Outreach website subscribers, as well as from Commonwealth and State agencies.
- We increased partner understanding of the threat from political interference at all levels of government through defensive briefings to reduce vulnerabilities in electoral systems and candidates, and through our advice to the Electoral Integrity Assurance Taskforce. We published assessments on espionage and foreign interference threats to the federal election and a state jurisdiction. This has supported more robust and resilient political systems and election processes.

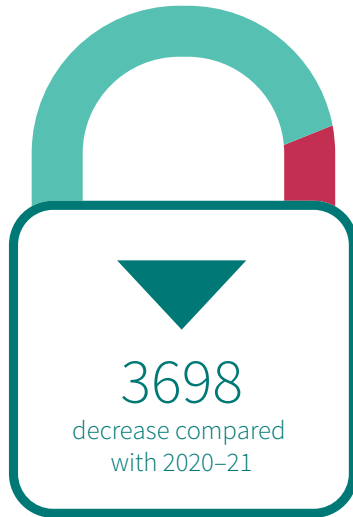
- During 2021–22, ASIO shared international connections and security and intelligence expertise to build Defence and National Intelligence Community (NIC) understanding of the impact of AUKUS arrangements on the security environment and threat to AUKUS capabilities. We will continue to leverage our international partnerships to determine NIC resource and capability commitments required to support AUKUS.
- ASIO raised awareness of the threat of espionage and foreign interference against Australia's critical infrastructure sectors through a range of briefings and products during this period. This included engagement with members of the Banking and Finance Sector Group and the Communications Sector Group to improve understanding of the espionage and foreign interference threat to key decision-makers, offshore facilities and supply chains.

Our personnel security assessments continued to play a pivotal role in assisting the Australian Government to manage threats to Australia's national security associated with access to privileged government information, places, activities and capabilities.

- In 2021–22, ASIO finalised 35 622 personnel security assessment referrals, comprising 31 381 assessments for Baseline, Negative Vetting (NV) 1 and 2 clearances and 4241 assessments for Positive Vetting (PV) clearances. The 2021–22 figure is a slight reduction on the 39 320 assessments finalised in 2020–21.

35 622

personnel security
assessment referrals



4241

assessments for
Positive Vetting (PV) clearances

31 381

assessments for Baseline,
Negative Vetting (NV) 1 and 2
clearances

During the reporting period, ASIO provided the following:



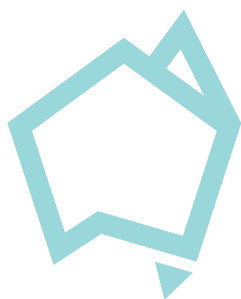
160

counter-espionage
and foreign interference
products



88

products that span both
counter-terrorism and
counter-espionage and
foreign interference



Border security

ASIO has continued to support whole-of-government efforts to protect Australia's border integrity. The Organisation has provided analysis of, and security advice on people smuggling activities, complex visa applications, and other movements of goods and people. This has assisted our partners to maintain the integrity of Australia's border protection programs.

Border security

Result—impact of ASIO’s border security operational activities advice

5. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our advice on countering serious threats to Australia’s border integrity, security-sensitive areas or substances had a MEDIUM impact on their decision-making in relation to actions and activities to disrupt and defend against serious threats to Australia’s border integrity, security-sensitive areas or substances.		
Target (2021–22)	70%; MEDIUM	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.18) PBS 2021–22, Outcome 1 (table 2.1.2)		
2021–2022 result		2020–2021 result	
38% HIGH; 56% MEDIUM		100% MEDIUM or higher (target: 70% MEDIUM)	

Stakeholder survey results show that 38 per cent of stakeholders rated ASIO’s performance against ASIO’s ‘border security—impact of operational activities’ advice as **HIGH**. A further 56 per cent of stakeholders rated ASIO’s impact as **MEDIUM**.

These results exceeded targets set in the *ASIO Corporate Plan 2021–25*, and demonstrated a similar performance against this measure to those in our 2020–21 results.

Reporting received throughout the year demonstrated ASIO’s support to whole-of-government border integrity activities.

Examples demonstrating ASIO’s impact on stakeholder policy development include the following.

ASIO’s advice provided context, was relevant and practical, and influenced decision-making

- ASIO tactical intelligence assessments informed Operation Sovereign Borders (OSB) assessments and decision-making in relation to people smuggling lead reporting.
- In this period, our assessments provided context for National Intelligence Community (NIC) partners in relation to people smuggling lead reporting. OSB provided positive feedback in relation to ASIO’s support.

ASIO finalised 6474 visa security assessments for the 2021–22 financial year, with 2493 (nearly 40 per cent) of those having been finalised between March and June 2022 (inclusive). This was on par with the 5971 assessments finalised in 2020–21.

Table 1: Completed visa assessments

Type of referral	2019–20	2020–21	2021–22
Temporary visas	589	506	320
Permanent residence and citizenship	49	24	43
Onshore protection (air)	8	7	8
Offshore refugee/humanitarian	115	43	6
Illegal maritime arrivals	14	4	3
Other referred caseloads	1740	909	961
Resolution of national security border alerts	8530	4478	5133
Total	11 045	5971	6474

Result—impact of ASIO’s border security policy development advice

6. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our advice on countering serious threats to Australia’s border integrity, security-sensitive areas or substances had a MEDIUM impact on their decision-making in relation to policy development and responses to serious threats to Australia’s border integrity, security-sensitive areas or substances.		
Target (2021–22)	70%; MEDIUM	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.19) PBS 2021–22, Outcome 1 (table 2.1.2)		
2021–2022 result		2020–2021 result	
42% HIGH; 42% MEDIUM		100% MEDIUM or higher (target: 70% MEDIUM)	

Stakeholder survey results show that 42 per cent of stakeholders rated ASIO’s performance against ASIO’s ‘border security—impact of policy development advice’ as **HIGH**. 42 per cent of stakeholders rated ASIO’s impact as **MEDIUM**.

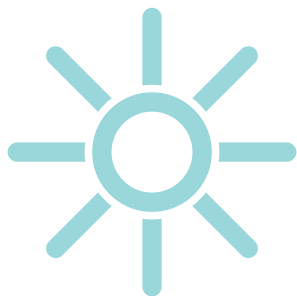
These results exceeded targets set in the *ASIO Corporate Plan 2021–25* and were similar to the result achieved against this measure in 2020–21.

Reporting received throughout the year demonstrated ASIO’s support to whole-of-government border integrity activities.

Examples demonstrating ASIO’s impact on border security operational activities advice include the following.

ASIO’s advice provided context, was relevant and practical, and influenced decision-making

- ASIO’s advice to the Department of Home Affairs provided relevant and practical input to assist Home Affairs strategic assessments relating to people smuggling via aviation stream networks.
- ASIO’s assessment product was sought by National Intelligence Community (NIC) partners to provide context on the people smuggling threat environment.



Capability program

ASIO is committed to accelerating our ability to achieve our purpose, deliver against our priorities and position the Organisation to meet future challenges. Through a human-led, data-driven, technology-enabled approach, our capability program aims to address capability gaps, keep ASIO in step with technological change, and maintain our ability to detect the early signs of threat activity. The program supports our ability to invest in, and sustainably adopt, new technology and tradecraft practices. This will include partnering with the Australian technology sector in the development of sovereign capabilities in key areas of national security, and further cementing our contribution to, and ongoing benefit from, our strategic partnerships. Improved application of commercial technologies will enable a more agile and sustainable response to changes in the rapidly evolving technology environment.

ASIO capability program

Result—ASIO capability program

7. ASIO capability delivery

Measure	The capability program delivers mission effects and outcomes through achieving deliverables consistent with capability program objectives and milestones.		
Target (2021–22)	Qualitative and quantitative measures demonstrate delivery of capability program milestones across the period.	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.20)		

In 2021–22, ASIO commenced a major capability uplift program, aimed at accelerating our ability to achieve ASIO’s purpose, deliver against our priorities, and position the Organisation to meet future challenges. The capability program was enabled by the significant investment made by government in 2021.

The capability program priority reflects a multi-year, multi-disciplinary program which supports ASIO’s ability to invest in, and sustainably adopt, new technology and tradecraft, in partnership with the Australian technology sector. The program is focused on addressing capability gaps, keeping ASIO in step with technological change, and maintaining our ability to detect threats at their earliest stage.

The first year of the program was planned to ensure the establishment of enduring foundations, with a significant focus on program governance and documentation. Eleven projects were initiated this year, with some initial milestone deliverables achieved.

Performance methodology for the capability program has focused on four inputs: program governance, program documentation, program milestones, and program deliverables and benefits. These four inputs were assessed as on-track as at the end of the 2021–22 reporting period.

A First Stage Gateway Review of the capability program was completed in early February 2022 and identified challenges at the organisational, portfolio, program and project level. With specialist external support from industry partners, program milestones and internal governance demonstrates that all elements of the capability program were on-track by the end of the 2021–22 reporting period.

Milestones and developments against the capability program measured during 2021–22 include the following.

Program governance

- Established the Capability Program Board as the senior oversight body, chaired by the Director-General of Security and including external members.
- Established a Program Management Office to provide program coordination, progress reporting, and prepare consolidated reporting.
- Established internal governance oversight for the capability program through a dedicated sub-committee of ASIO's Capability Investment Committee (CIC), chaired by ASIO's Deputy Director-General Enterprise Service Delivery, who is the program's Senior Responsible Officer (SRO).
- Established individual project boards to coordinate resourcing, scheduling, risks and issues, and project interdependencies.

- Introduced two sub-program governance bodies, to be implemented from 1 July 2022, which will oversee alignment and interdependency of specific projects with ongoing capability management and delivery.
- Established partnerships with industry to support, evolve and improve portfolio, program and project management approaches.
- Identified an Independent Program Assurance Capability to provide independent oversight and advice to the program SRO.

Program documentation

- Established program and project reporting and artefacts, refined through the CIC and embedded within a monthly reporting cycle.
- Documentation has reliably reported budget, scope and schedule progress at both the program and project level.
- Established project proposals for each project over the first four years of the capability program. Proposals assign responsibilities for delivery and establish the foundations for progress measurement.
- Established risk reporting at project and program level which is reviewed monthly.
- Engaged a change management specialist to ensure key stakeholders are engaged in the change process and deliver a change management approach.
- Program documentation continues to be refined to track progress, outcomes and areas of focus.

Program milestones

- Since commencement, the program has met the majority of milestones set at the time of program design, with a small number of projects receiving approved extensions to schedules. The shifts should not impact key project deliverables or the realisation of program benefits.

Program deliverables and benefits

- Undertook stakeholder workshops to discuss and map program benefits.
- Benefits identified for all active projects supported by the development of benefit profiles and baselines.
- Project benefit metrics continue to be defined and introduced, with ongoing work carrying across to the next reporting period.



Risk and compliance

Accepting and engaging with risk is inherent to our role to protect Australia and Australians from threats to their security. In a complex security environment, our risk and compliance frameworks enable informed decision-making and effective prioritisation. ASIO officers act with integrity. We are impartial, committed to our purpose, and operate ethically and with propriety. Our frameworks support our compliance with the law and enable dynamic responses to our evolving threat environment.

Risk and compliance

Result—risk and compliance

8. Risk management framework

Measure	ASIO’s risk management framework, culture and practices are consistent with the requirements of the Commonwealth Risk Management Policy.		
Target (2021–22)	Adherence to the requirements of the Commonwealth Risk Management Policy in order to identify and manage risk, and drive a compliance culture.	Outcome	ACHIEVED
Source	ASIO Corporate Plan 2021–25 (p.21)		

Maintaining an appropriate system of risk oversight and management ensures ASIO can fulfil its purpose—to protect Australia and Australians from threats to their security. Our enterprise risk management framework ensures we engage with risk in all aspects of our business, and apply a sophisticated understanding of risk management practices to identify, evaluate and respond to risks and opportunities.

ASIO’s framework includes the following documents, approved by the Director-General as ASIO’s accountable authority:

- The Risk Management Policy, which defines the Organisation’s approach to the management of risk, supports its strategic direction, articulates key roles and responsibilities for managing risk within ASIO and includes the processes and tools which embed risk management into business processes.

- The Risk Appetite and Tolerance Statement, which establishes the Organisation’s approach to risk, guides the nature and level of risk ASIO is willing to accept to achieve its objectives, and helps establish a strong risk management culture.
- The Enterprise Risk Register, which records ASIO’s enterprise risks, their ratings and how they are managed.

Key outcomes

In 2021–22, ASIO maintained compliance with all elements of the Commonwealth Risk Management Policy, demonstrating our commitment to an appropriate system of risk oversight and management.

- ASIO matured the risk framework in the areas of practice, procedure, culture and leadership. Processes were refined, supporting accountability and transparency, with a collaborative approach to risk. This included:
 - progressing integration with the enterprise compliance framework, bringing greater awareness of compliance risks;
 - reviewing the language in the list of accountabilities and responsibilities to ensure that staff responsibilities are appropriately defined; and
 - developing an education package to further support and assist staff in their implementation of the enterprise risk management framework.
- ASIO conducted dedicated senior executive discussions on contemporary thinking about enterprise risk management, focusing on embedding a shared understanding of risk across the Organisation, linking day-to-day decisions with enterprise risk.
- ASIO's risk and compliance culture is identified as a key element in our enterprise risk management framework, supported by the senior executive leadership who sets risk appetite and tolerance. Strategic engagements were conducted across a wide range of internal stakeholders, promoting an open and proactive approach to managing, reporting and communicating risk.
- All ASIO divisions assessed and reported risk across ASIO's six risk categories (legal and propriety, financial, capability, security, health and safety, reputation). Risk and compliance templates were refined to ensure assessments and reporting highlighted the consideration of ASIO's risk tolerance thresholds across these six categories. Divisional Risk Registers were mapped to the Enterprise Risk Register, reflecting the top down and bottom up approach to ASIO's enterprise risk management framework.
- Policies and procedures within the Organisation were reviewed to align with the risk framework and consider ASIO's risk appetite and tolerance thresholds. For example, risk management has been incorporated into business processes to support the Crisis Management Team to manage transition arrangements to 'COVID-normal' in each of the states and territories.

Report on financial performance

The 2021–22 financial statements report a \$94.1 million operating deficit compared with an \$82.2 million operating deficit the previous financial year. ASIO's 2021–22 operating funding from government was \$480.3 million compared to \$455.2 million in 2020–21. In 2021–22 ASIO incurred \$140.7 million in depreciation and amortisation expenses (including for the right-of-use leased assets) noting that the Australian Government does not provide operating funding for these expenses. ASIO also incurred \$34.7 million in principal repayments for leased assets reflecting the implementation of Australian Accounting Standards Board Standard 'Leases' (AASB 16 Leases) which became effective on 1 July 2019. After adjusting for these items, the 2021–22 operating result is a surplus of \$11.9 million compared to \$25.6 million in 2020–21. This surplus includes \$11.5 million as a result of the impact of movements in government bond rates on the valuation of employee leave provisions.

In 2021–22 ASIO received \$87.0 million in capital funding through the departmental capital budget for asset replacement and equity injections. This compares to \$92.7 million in 2020–21. 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.

A table summarising ASIO's total resources for 2021–22 is provided at **Appendix A**.

Our total expenses by outcome for this reporting period are at **Appendix B**.

5



An aerial photograph of a university campus. In the center is a large, white, rectangular building with many windows. In front of it is a red running track and a circular area with a fountain. The campus is surrounded by green lawns and trees. The image has a teal gradient overlay at the top.

5

MANAGEMENT AND ACCOUNTABILITY

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).

The Director-General is supported by a number of corporate governance committees, including ASIO's peak governing body (the Executive Committee); three internal advisory committees (the Security and Compliance Committee, the Capability and Investment Committee, and the Influence and Impact Committee); and an independent advisory committee (the Audit and Risk Committee).

Throughout 2021–22, ASIO continued to refine its enterprise management and governance practices, including by:

- reviewing ASIO's approach to enterprise risk management and establishing a comprehensive work plan to mature risk management practices against the Commonwealth Risk Management Maturity Model;
- continuing updates to ASIO's business continuity framework, supported by dedicated crisis management guidance materials, to ensure the Organisation is positioned to sustain high-priority operations in the event of a significant disruption; and
- establishing the Influence and Impact Committee to drive matters relating to or impacting ASIO's influence agenda, and to give account of performance against ASIO's objectives and endorsed lines of effort.

Executive Committee

The Executive Committee is ASIO's peak governing body, advising the Director-General on matters requiring executive decision-making. The Executive Committee's purpose is to provide oversight of all ASIO activities, including the effective management of ASIO's risks. The Executive Committee sets and reviews the Organisation's risk appetite and tolerance, determines whether ASIO's overall level of risk is acceptable, and considers whether the risk management framework remains effective.

Security and Compliance Committee

The Security and Compliance Committee, chaired by Deputy Director-General Intelligence Service Delivery, makes recommendations to the Executive Committee on significant security and compliance matters relating to or impacting ASIO, including the successful delivery of ASIO's strategic objectives and management of enterprise risk.

Capability and Investment Committee

The Capability and Investment Committee, chaired by the Deputy Director-General Enterprise Service Delivery, makes recommendations to the Executive Committee on significant matters relating to organisational capability and investment and ensures their alignment to ASIO’s strategic objectives.

Influence and Impact Committee

The Influence and Impact Committee, chaired by the Principal Advisor, makes recommendations to the Executive Committee on significant matters relating to or impacting on ASIO’s influence agenda and gives account of performance against ASIO’s objectives and endorsed lines of effort.



Figure 2: ASIO’s governance framework

ASIO's response to COVID-19

ASIO continued to mature its response to COVID-19 to ensure continued coverage of high-priority targets related to our counter-terrorism and counter-espionage and foreign interference missions.

From the onset of the COVID-19 pandemic, ASIO's COVID-19 response was led by the ASIO Crisis Management Team (CMT). The CMT managed ASIO's posture to the pandemic, ensuring compliance with public health directions while applying mitigations to potential impacts on staff and daily operations. To reduce the risk of exposure to COVID-19 within the workplace, the CMT oversaw the implementation of adaptive working arrangements for staff and supported transition to 'COVID-normal' arrangements.

Acknowledging the evolving nature of the COVID-19 environment, responsibility for continuing oversight and action transitioned to a new COVID-19 Coordination Team (CCT), chaired by the Deputy Director-General Enterprise Service Delivery, in December 2021. Since that time, the CCT has been leading the way for ASIO to resume a 'COVID-normal' way of working.

The CCT continues to monitor the COVID-19 environment, ensuring ASIO remains agile in ensuring workforce safety and business continuity.

External scrutiny

Parliamentary Joint Committee on Intelligence and Security

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

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

In 2021–22, ASIO provided a written submission to the PJCIS Review of Administration and Expenditure No. 20 (2020–21). Beyond administration and expenditure, ASIO also contributed to a number of PJCIS reviews and inquiries, including:

- the review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021;
- the review of the *Counter-Terrorism (Temporary Exclusion Orders) Act 2019*;
- the review of the *Foreign Influence Transparency Scheme Act 2018*;
- the review of the Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020; and
- reviews of the listing and relisting of terrorist organisations.

Senate Legal and Constitutional Affairs Committee

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate Estimates process on 25 October 2021, 14 February 2022 and 31 March 2022.

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 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 IGIS 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 has 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 2021–22 the IGIS regularly inspected activities across our operational functions and investigated any complaints received by the Office. We are committed to acting with legality and propriety, and in 2021–22 we continued to take action 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) independently reviews the operation, effectiveness and implications of national security and counter-terrorism laws; and considers whether the laws contain appropriate protections for individual rights, remain proportionate to terrorist or national security threats, and remain necessary.

In conducting reviews the INSLM has access to all relevant material, regardless of national security classification, can compel answers to questions, and holds public and private hearings. INSLM reports are tabled in Parliament.

During 2021–22, ASIO made a submission to the INSLM on their review into Division 105A of the *Criminal Code Act 1995* (Cth).

Independent Reviewer of Adverse Security Assessments

The Independent Reviewer of Adverse Security Assessments (Independent Reviewer) reviews adverse ASIO security assessments that impact individuals who are in immigration detention and who have been found by Home Affairs to be owed protection under international law. The Independent Reviewer conducts a primary review of each adverse security assessment. For eligible individuals, these assessments are periodically reviewed—every 12 months—for the duration of the adverse assessment.

Appendix C provides the Independent Reviewer's annual report for the 2021–22 reporting period.

Compliance

Ethical behaviour and integrity are core values of the Organisation, and are essential to sustaining 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 our centralised compliance function and internal assurance frameworks continued to strengthen, and ASIO commissioned an independent review of the maturity of the compliance function. The review found the centralised compliance function has played an important role in improving ASIO's compliance.

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 systems of internal control.

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 2014*.¹

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.² The committee members have a broad range of appropriate qualifications, knowledge, skills and experience relevant to the operations of ASIO. This includes at least one member with accounting or related financial management experience, and 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 Audit and Risk Committee met five times (four quarterly meetings and an extraordinary meeting convened for the financial statements review) with each meeting having a quorum.

Fraud control and management

ASIO has zero tolerance for fraudulent behaviour. ASIO treats both suspected and actual fraud seriously and takes all reasonable measures to prevent, detect and investigate fraudulent behaviour.

The *ASIO Fraud Control Plan 2021–23* documents our approach to fraud awareness, prevention, detection, reporting and investigation, and our commitment to ensuring efficient, effective and ethical use of resources. This includes 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 2017*.

During the reporting period ASIO conducted fraud pressure testing on a sample of countermeasures (also known as controls) identified in our Fraud Risk Assessment. This allowed us to identify fraud vulnerabilities and determine the effectiveness of our countermeasures.

As part of this framework, all staff must complete mandatory e-Learning on ethics and accountability, including modules on fraud, during induction and then at least every three years thereafter.

The *ASIO Fraud Strategy Statement 2021* (www.asio.gov.au/resources/strategy-and-policy/asio-fraud-strategy-statement) provides further information on our fraud control and management arrangements.

¹ Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, a direct electronic address for the charter determining the functions of ASIO's Audit and Risk Committee has been deleted from the version of the Annual Report 2021–22 tabled in Parliament. (**Appendix R**)

² Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, membership and remuneration details have been deleted from the version of the Annual Report 2021–22 tabled in Parliament. (**Appendix R**)

Significant legal matters affecting ASIO's business

During 2021–2022 ASIO continued to be involved in numerous legal proceedings in courts and tribunals. Matters have included prosecutions, judicial and merits review matters, coronial inquests and civil proceedings.

Administrative Appeals Tribunal

ASIO was involved in proceedings before the Administrative Appeals Tribunal (AAT). Most of these proceedings were reviews of ASIO security assessments. There were 16 reviews of ASIO security assessments active in 2021–2022. These ASIO security assessments relate to eligibility for passports, visas, security clearances, citizenship and the use and supply of telecommunications carriage services.

Over the reporting period, ASIO also assisted the AAT in four reviews of National Archives access decisions in which exemptions had been claimed to protect ASIO material from release.

AAT decisions are reported on the Australasian Legal Information Institute (AustLII) website (www.austlii.edu.au).

Criminal prosecutions, coronial inquests and civil proceedings

In collaboration with our law enforcement partners and prosecuting authorities—and with appropriate protections—ASIO provided information for use as evidence, and responded to subpoenas and disclosure requests in a number of criminal prosecutions. ASIO has also provided information to assist coroners in inquests and has been a respondent to one civil claim.

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 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. Executive remuneration is discussed at **Appendix D**.

The salary ranges available for employees by classification level are shown at **Appendix E**.

Performance management

The ASIO Performance Management Framework supports the development of the skills and capability required to achieve the Organisation's strategic and operational goals.

Consistent with policy requirements, all ASIO employees participated in the 2021-22 performance management cycle.

ASIO's Performance Management Framework was revised in 2021 to support increased employee engagement and improve the quality of performance and development discussions through closer alignment of performance expectations, career goals and development needs. The framework includes career conversations and aims to support talent through relevant learning experiences.

ASIO's ongoing commitment to support and develop our leaders through manager-once-removed feedback continues to be incorporated into the performance management conversations.

People strategy

ASIO continued to implement its five-year *Workforce Plan 2025* to ensure the Organisation is well positioned to meet current and future workforce challenges. The three key areas of focus outlined in the plan are capability, efficiency and engagement.

Actions completed in the second year of the plan included:

- embedding the People Capability Framework through the Organisation's people processes;
- conducting a work and workforce redesign pilot to target the key areas of capability, efficiency and engagement in the workplace;
- conducting an all-staff pulse check survey; and
- developing an updated staff mobility policy.

These deliverables support the ongoing professional development, retention and engagement of staff.

Diversity and inclusion

ASIO continues to be committed to a diverse and inclusive work environment where all employees are valued and respected, and can reach their full potential as part of a highly capable, innovative and adaptive workforce. We know that inclusion fosters innovation and creativity, and increases productivity. It increases employee satisfaction and retention, and ensures our people are physically and psychologically safe. Inclusion promotes equal opportunity and supports our people to be their best.

The *Diversity and Inclusion Strategy 2021–24* is the roadmap for prioritising action and monitoring the progress of our diversity and inclusion objectives. The progress of diversity and inclusion was reflected in our staff survey where 90 per cent of staff support diversity and inclusion within ASIO.

ASIO's commitment to inclusion has continued to mature, particularly in respect of disability support, and in the past few years our CapABILITY network has been an influential advocate towards disability awareness and inclusion. This has culminated in the development and launch of ASIO's *Disability Action Plan* (2022–2024). The plan clearly sets out ASIO's intention to create a workplace that is more inclusive of people with disability, or disability-related caring responsibilities, and recognises the tangible benefits to ASIO's outcomes.

ASIO has also delivered against its commitment on its initial *Reconciliation Action Plan* (RAP) in 2022. The RAP was pivotal in providing greater awareness of the importance of our Indigenous history and the role that all employees play in reconciliation in ASIO.

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

ASIO's seven staff-led diversity networks form an essential part of creating a diverse and inclusive culture. Our networks empower individuals to initiate change and work together to achieve our diversity and inclusion goals.

The ASIO Diversity and Inclusion Council provides oversight of the diversity networks, strategic alignment of diversity activities and annual reporting of network outcomes.

Diversity networks

aGENda

Our gender-equity network promotes equal opportunity for the ASIO workforce, regardless of gender. The aGENda network organises events and initiatives to ensure gender equity considerations continue to shape the corporate agenda. The aGENda network is committed to tangible outcomes through policy reform, awareness raising, research, advocacy and engagement with government for improved gender equity outcomes across the national security community.

ASIOpen

Our gender and sexually diverse network promotes an inclusive workplace culture and supports gender and sexually diverse employees to be open and authentic in the workplace. ASIOpen celebrates the benefits of inclusivity and drives reform on gender and sexually diverse issues through information sharing, hosted events and policy reform.

CapABILITY

Our CapABILITY network represents staff experiencing all forms of physical and mental health issues, neurodiversity and caring responsibilities. CapABILITY advocates for increased awareness, acceptance and respect for all forms of ability within ASIO. CapABILITY works in ASIO to overcome barriers to staff access and participation within ASIO's physical environment and to promote the acceptance and celebration of neurodiversity within the Organisation.

Introverts

Our introverts network contributes to all staff being heard, recognised and valued for their contributions, regardless of how introverted or extroverted they are. The network champions diversity in thinking and communication style, and contributes to a positive workplace culture by progressing improvements to ASIO's policies and procedures to support introverted employees to reach their full potential.

Mozaik

Our Mozaik network is ASIO's cultural and linguistic diversity network. Mozaik advocates for, and on behalf of, ASIO's culturally and linguistically diverse workforce, and collaborates with staff and management to develop tangible work programs to remove potential barriers to acceptance, and opportunity.

Mudyi

ASIO acknowledges the traditional owners of this land and pays respect to elders past, present and emerging. Our Aboriginal and Torres Strait Islander network is committed to supporting reconciliation by fostering a culture where diversity is appreciated and supported, and which contributes to the coming together of Australians in an equal and inclusive society. Mudyi helps drive corporate initiatives that support diversity and improve the workplace experience for Indigenous Australian people.

Parents' Network

This network is for ASIO staff who are parents, or who are about to become parents, and helps parents—both while they are on leave and as they return to work—to navigate flexible and part-time working arrangements.

ASIO Ombudsman

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

During the reporting year, the ASIO Ombudsman supported employees and line managers through:

- informal discussions;
- input and discussions on training documents and general policy application; and
- information-sharing, such as best-practice policy and research papers.

In addition, the following formal engagements occurred:

- three staff requests on the application of the COVID-19 vaccine policy;
- completion of two staff reviews;
- five inquiries into staff concerns; and
- discussions with staff networks.

In 2021–22 the ASIO Ombudsman did not undertake any public interest disclosure reviews; however, advice on public interest disclosure procedures was provided.

Asset management

The Organisation's governance framework for managing assets so that asset balances in the financial statements are accurately reported includes:

- asset investment and replacement, through setting an annual budget that reflects both government priorities and ongoing business requirements. The budget is monitored monthly and reviewed regularly during the year to ensure planned expenditure reflects business requirements;
- undertaking a rolling annual stocktake, impairment review and useful life expectancy review to update and verify the accuracy of asset records;
- conducting fair-value measurement through three-yearly revaluations of all tangible assets, which is completed by qualified external valuers. A materiality review is undertaken in the years between valuations;
- maintaining property, plant and equipment assets through maintenance programs; and
- providing a centralised procurement policy and advice service, including quality control oversight.

Purchasing

During 2021–22 ASIO adhered to the Commonwealth Procurement Rules (CPR) and associated policy and guidelines. ASIO's compliance was monitored by the Audit and Risk Committee as well as the Security and Compliance Committee. No significant issues were identified and overall compliance was acceptable.

Annual reports contain information about actual expenditure on reportable consultancy contracts. Information on the value of reportable consultancy contracts is available on the AusTender website. Annual reports contain information about actual expenditure on reportable non-consultancy contracts. Information on the value of reportable non-consultancy contracts is available on the AusTender website. ASIO is not required to publish information on the AusTender website, in line with authorised exemptions to avoid prejudice to essential security interests. A list of consultancy and non-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 to the PJCIS on request, which oversees our administration and expenditure.

Consultancies

ASIO 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.

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

As shown in table 2, during 2021–22, 20 new consultancy contracts were entered into involving total actual expenditure of \$8.8 million. In addition, 15 ongoing consultancy contracts were active during the period, involving total actual expenditure of \$2.9 million.

Table 2: Expenditure on consultancy contracts for the current reporting period (2021–22)

	Number	Expenditure \$'000 (GST inc.)
New contracts entered into during the reporting period	20	8823
Ongoing contracts entered into during a previous reporting period	15	2966
Total	35	11 789

Table 3: Expenditure on non-consultancy contracts for the current reporting period (2021–22)

	Number	Expenditure \$'000 (GST inc.)
New contracts entered into during the reporting period	409	112 196
Ongoing contracts entered into during a previous reporting period	224	75 196
Total	633	187 392

Non-consultancy contracts

As shown in table 3, in the 2021–22 reporting period ASIO entered into 409 new non-consultancy contracts at a value of \$112.2 million, and in addition, 224 ongoing non-consultancy contracts at a value of \$75.2 million were active during the reporting period.

Australian National Audit Office access clauses

During this reporting period, ASIO 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 to the PJCS on request.

Procurement initiatives to support small business

ASIO 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 www.finance.gov.au.

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 and responses; and
- using electronic systems to facilitate the Department of Finance's Procurement On-Time Payment Policy for Small Business, including payment cards.

ASIO 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 the Treasury's website.

Other mandatory information

Advertising and market research

During 2021–22, ASIO conducted the following advertising campaigns: recruitment and marketing. Further information on these advertising campaigns is available at 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

Australia's Disability Strategy 2021–2031 (the Strategy) is the overarching framework for inclusive policies, programs and infrastructure that will support people with disability to participate in all areas of Australian life. The Strategy sets out where practical changes will be made to improve the lives of people with disability in Australia. 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 have committed to deliver more comprehensive and visible reporting under the Strategy. A range of reports on progress of the Strategy's actions and outcome areas will be published and available at www.disabilitygateway.gov.au/ads.

Appendix F of ASIO's annual report provides information on the diversity of our workforce, including statistics on people with a disability. The annual report is also available at www.asio.gov.au.

Commonwealth Child Safe Framework—statement of compliance

ASIO has a strong commitment to child safety, protecting and safeguarding children, while promoting and maintaining a culture that provides a safe environment for children.

ASIO's purpose is to protect Australia and Australians from threats to their security. In meeting this purpose, ASIO has occasional contact with minors, including direct and indirect contact.

An annual risk assessment of ASIO's roles and activities has been undertaken to ensure that existing and emerging risks to children are identified and addressed. It was assessed that risks to the safety of children and young people as a result of ASIO's activities has a rare likelihood of occurrence (with effective mitigations in place). The overall risk to the safety of children and young people in 2021–22 was assessed as medium.

ASIO's activities are consistent with each of the four requirements of the Commonwealth Child Safe Framework (CCSF). Further, ASIO's operational and investigative activity involving children is managed through the application of laws and policies to support children's physical and psychological safety, the maintenance of a workforce that is appropriately trained, qualified and compliant with mandatory obligations, and the effective identification, reporting and management of child-related incidents. In addition, strong safeguards are embedded in legislation relating to the compulsory questioning of minors under the *ASIO Act 1979*. Staff are aware of the sensitivities that apply when working with children and have access to specialist advice as required.

By complying with the requirements of the CCSF, adhering to ASIO's policies and procedures, and identifying and controlling the identified child-related risks, the possibility of harm to children is mitigated.

ASIO's review of child-related risks during 2021–22 will be used to further refine policies and procedures, and improve staff awareness.

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* (Archives Act). This provides for public access to Commonwealth records in the 'open period'. The current open period covers all Commonwealth records created before 2002. ASIO works closely with the National Archives of Australia to facilitate access to ASIO records.

During the reporting period, ASIO received 256 requests for access to ASIO records, and completed a total of 239 requests, equating to 42 037 pages requiring assessment.

The lower number of requests completed within 90 days 2021–22 is due in part to:

- the allocation of resources to complete a number of requests with a high volume of content;
- a significant allocation of resources to assist with an AAT case; and
- a decrease in available resources to undertake assessments.

Table 4: Access to ASIO records

	2017–18	2018–19	2019–20	2020–21	2021–22
Applications for record access	345	344	334	537	256
Requests completed	310	410	399	538	239
Pages assessed	36 312	57 783	72 820	47 913	42 037
Percentage of requests completed within 90 days	66.7%	60%	59%	79%	53%

Australian Security Intelligence Organisation Act 1979

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

The statement on questioning warrants is provided at **Appendix J**. To ensure compliance with section 94 of the ASIO Act, and to avoid prejudice to security, the Minister for Home Affairs, on advice from the Director-General of Security, has made deletions from the annual report tabled in Parliament. The following deletions have been made under section 94(5) of the ASIO Act; **Appendix L** relating to special intelligence operation authorities, **Appendix M** relating to authorisations for access to telecommunications data,

Appendix N relating to use of technical assistance requests, technical assistance notices and technical capability notices, **Appendix O** relating to use of special powers under warrant and other powers, and **Appendix P** relating to applications for international production orders.

These appendices are provided separately to the Minister for Home Affairs and, as required by the ASIO Act, to the Leader of the Opposition.

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 reports 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 2021–22 is provided at **Appendix H**.

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 2021–22 is provided at **Appendix I**.

6



A low-angle, upward-looking photograph of a modern building's interior. The image features multiple levels with glass railings and concrete balustrades. The architecture is characterized by sharp, geometric lines and a color palette of teal, grey, and warm yellow. A large, stylized number '6' is overlaid in the top right corner. The text 'FINANCIAL INFORMATION' is centered in the middle of the image.

6

FINANCIAL INFORMATION

Financial information

ASIO prepared financial statements for the year ended 30 June 2022 that 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. These financial statements have been audited by the Australian National Audit Office (ANAO) who have issued an unmodified audit opinion.

The audited financial statements together with the ANAO audit opinion and the Statement by the Director-General of Security have been provided to the Minister for Home Affairs as required by subsection 43(1) of the PGPA Act, through their inclusion in the classified Appendices to the ASIO Annual Report 2021–22 (**Appendix Q**).

For national security reasons the financial information provided in this Annual Report has been summarised into higher-order categories and detailed notes have been removed, as allowed by the application of section 105D of the PGPA Act.

CONTENTS

STATEMENT OF COMPREHENSIVE INCOME	97
STATEMENT OF FINANCIAL POSITION	98
STATEMENT OF CHANGES IN EQUITY	99
STATEMENT OF CASH FLOWS	100
NOTES TO THE FINANCIAL STATEMENTS	101
Overview	101
1. Financial performance	102
1.1 EXPENSES	102
1.2 OWN-SOURCE REVENUE	102
2. Financial position	103
2.1 FINANCIAL ASSETS	103
2.2 NON-FINANCIAL ASSETS	103
2.3 PAYABLES	105
2.4 INTEREST BEARING LIABILITIES	105
2.5 PROVISIONS	105
3. Funding	106
3.1 APPROPRIATIONS	106
4. Managing uncertainties	107
4.1 CONTINGENT ASSETS AND LIABILITIES	107
4.2 FINANCIAL INSTRUMENTS	107
5. Other information	108
5.1 CURRENT/NON-CURRENT DISTINCTION FOR ASSETS AND LIABILITIES	108
5.2 KEY MANAGEMENT PERSONNEL REMUNERATION	108
5.3 RELATED PARTY DISCLOSURES	109
5.4 MAJOR BUDGET VARIANCES	110

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

STATEMENT OF COMPREHENSIVE INCOME

for the period ended 30 June 2022

	Notes	2022 \$'000	Original budget 2022 \$'000	2021 \$'000
EXPENSES	1.1	596 686	615 237	554 071
OWN-SOURCE INCOME	1.2			
Revenue		17 883	24 579	16 281
Gains		4437	145	369
<i>Net cost of services</i>		<i>(574 366)</i>	<i>(590 513)</i>	<i>(537 420)</i>
REVENUE FROM GOVERNMENT	3.1	480 266	475 602	455 198
DEFICIT ON CONTINUING OPERATIONS		(94 100)	(114 911)	(82 222)
OTHER COMPREHENSIVE INCOME		(5)	-	-
TOTAL COMPREHENSIVE LOSS		(94 105)	(114 911)	(82 222)

STATEMENT OF FINANCIAL POSITION

as at 30 June 2022

	Notes	2022 \$'000	Original budget 2022 \$'000	2021 \$'000
ASSETS				
Financial assets	2.1	184 200	120 602	157 749
Non-financial assets	2.2	860 013	894 698	924 115
TOTAL ASSETS		1 044 213	1 015 300	1 081 864
LIABILITIES				
Payables	2.3	24 437	23 837	14 532
Interest bearing liabilities	2.4	553 165	563 498	587 065
Provisions	2.5	94 895	102 288	101 435
TOTAL LIABILITIES		672 497	689 623	703 032
NET ASSETS		371 716	325 677	378 832
EQUITY				
Parent equity interest				
Contributed equity		1 095 003	1 100 794	1 008 014
Reserves		90 369	90 373	90 374
Accumulated deficit		(813 657)	(865 490)	(719 556)
TOTAL EQUITY		371 716	325 677	378 832

STATEMENT OF CHANGES IN EQUITY

for the period ended 30 June 2022

	2022 \$'000	Original budget 2022 \$'000	2021 \$'000
RETAINED EARNINGS			
Opening balance	(719 556)	(750 579)	(637 334)
Comprehensive income			
Deficit for the period	(94 100)	(114 911)	(82 222)
Closing balance	(813 657)	(865 490)	(719 556)
ASSET REVALUATION RESERVE			
Opening balance	90 374	90 373	90 374
Other comprehensive income	(5)	-	-
Closing balance	90 369	90 373	90 374
CONTRIBUTED EQUITY			
Opening balance	1 008 014	1 008 014	915 296
Transactions with owners			
Contributions by owners			
Equity injection—appropriation	48 501	48 501	10 456
Departmental capital budget	38 488	44 279	82 262
Closing balance	1 095 003	1 100 794	1 008 014
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	371 716	325 677	378 832

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 2022

	2022	Original budget 2022	2021
	\$'000	\$'000	\$'000
OPERATING ACTIVITIES			
Cash received			
Appropriations	521 366	507 257	452 579
Other	40 016	41 714	36 474
Cash used	517 738	508 055	456 595
NET CASH FROM/(USED BY) OPERATING ACTIVITIES	43 644	40 916	32 458
INVESTING ACTIVITIES			
Cash received	195	-	417
Cash used	74 841	102 879	83 946
NET CASH FROM/(USED BY) INVESTING ACTIVITIES	(74 646)	(102 879)	(83 529)
FINANCING ACTIVITIES			
Cash received	74 220	95 702	82 839
Cash used	34 749	36 112	34 241
NET CASH FROM/(USED BY) FINANCING ACTIVITIES	39 471	59 590	48 598
Net increase (decrease) in cash held	8469	(2373)	(2473)
Cash and cash equivalents at the beginning of the reporting period	13 787	15 247	16 260
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD	22 256	12 874	13 787

NOTES TO THE FINANCIAL STATEMENTS

Overview

The basis of preparation

The financial statements underpinning this financial information 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* (FRR); and
- Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The underlying 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 information is presented in Australian dollars.

New accounting standards

There were no new or revised accounting standards that are applicable to the current reporting period.

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 position or performance of ASIO.

1. Financial performance

1.1 EXPENSES

Accounting policy

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.

1.2 OWN-SOURCE REVENUE

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.

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

2.1 FINANCIAL ASSETS

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

Credit terms for goods and services were within 30 days (2021: 30 days).

Financial assets were assessed for impairment at 30 June 2022.

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.

2.2 NON-FINANCIAL ASSETS

Impairment

Non-financial assets are assessed for impairment at the end of each reporting period. 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.

Accounting policy

Acquisition of assets

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

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.

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

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

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.

All assets were assessed for impairment at 30 June 2022. 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.

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 a qualified valuer to conduct a materiality review of carrying amounts for all non-financial assets (excluding software and lease right-of-use assets) as at 31 March 2022. The valuer 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.

2.3 PAYABLES

Settlement is usually made within 30 days.

2.4 INTEREST BEARING LIABILITIES

Accounting policy

For all new contracts entered into, ASIO considers whether the contract is, or contains a lease.

A lease is defined as 'a contract, or part of a contract, that conveys the right to use an asset (the underlying asset) for a period of time in exchange for consideration'.

Once it has been determined that a contract is, or contains, a lease, the lease liability is initially measured at the present value of the lease payments unpaid at the commencement date, discounted using the interest rate implicit in the lease, if that rate is readily determinable, or the Organisation's incremental borrowing rate. Subsequent to initial measurement, the liability will be reduced for payments made and increased for interest. It is remeasured to reflect any reassessment or modification to the lease. When the lease liability is remeasured, the corresponding adjustment is reflected in the right-of-use asset or profit and loss depending on the nature of the reassessment or modification.

2.5 PROVISIONS

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 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.

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.

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.

3. Funding

3.1 APPROPRIATIONS

3.1.A Annual departmental appropriations

	Ordinary annual services \$'000	Capital budget \$'000	Equity injections \$'000
2022			
Appropriation Act			
Annual appropriation	480 266	38 488	48 501
PGPA Act			
Section 74 transfers	37 723	-	-
Total appropriation	517 989	38 488	48 501
Appropriation applied (current and prior years)	(510 305)	(35 800)	(38 420)
Variance	7684	2688	10 081
2021			
Appropriation Act			
Annual appropriation	455 198	82 262	10 456
PGPA Act			
Section 74 transfers	19 099	-	-
Total appropriation	474 297	82 262	10 456
Appropriation applied (current and prior years)	(454 432)	(72 782)	(10 057)
Variance	19 865	9480	399

4. Managing uncertainties

4.1 CONTINGENT ASSETS AND LIABILITIES

Quantifiable liabilities

ASIO's contingent liabilities relate to claims for damages or costs. ASIO is defending the claims.

Unquantifiable contingencies

At 30 June 2022, 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

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

	2022	2021
	\$'000	\$'000

5.1 CURRENT/NON-CURRENT DISTINCTION FOR ASSETS AND LIABILITIES

Assets expected to be recovered in:

No more than 12 months	210 056	181 677
More than 12 months	834 157	900 187
Total assets	1 044 213	1 081 864

Liabilities expected to be recovered in:

No more than 12 months	88 347	41 626
More than 12 months	584 150	661 406
Total liabilities	672 497	703 032

5.2 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	2257	2047
Long-term employee benefits	117	144
Post-employment benefits	363	343
Total key management personnel remuneration expenses	2737	2534

The number of key management positions as at 30 June 2022 is 6 (2021: 5).

Membership of the Executive Committee changed throughout 2021–22. Several key management positions were occupied by different officers for portions of the year.

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.

5.3 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 2021–22 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.

5.4 MAJOR BUDGET VARIANCES

The following provides an explanation of variances between the original budget as presented in the 2021–22 Portfolio Budget Statements (PBS) and the 2021–22 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. The original budget as presented in the 2021–22 PBS may be amended by Government throughout the year. ASIO's budget for 2021–22 was updated as part of the 2021–22 Additional Estimates.

Expenses

Actual expenses are \$18.551 million (3%) lower than original budget reflecting:

- depreciation and amortisation expenses were lower than original budget due to delays in the timing of asset purchases;
- employee benefits were lower than original budget due to the impact of movements in the 10 year bond rate and the lower than anticipated staffing levels; and
- supplier expenses were higher than original budget primarily due to the level of operational activity.

Income

Income is \$2.260 million (<1%) higher than original budget reflecting:

- an increase of \$4.664 million in revenue from government as a result of an estimates variation at the 2021–22 Additional Estimates; and
- own source revenue was \$2.405 million less than budget. This budget is dependent on activities undertaken by external parties which was less than anticipated due to the ongoing impact of COVID–19.

Assets

Total assets are \$28.913 million higher (3%) than original budget. Financial assets are \$63.598 million higher than budget largely due to undrawn appropriation as a result of reduced expenditure through the year. These funds form part of the trade and other receivables balance and will be available in 2022–23.

Non-financial assets are \$34.685 million lower than original budget. The variance across all asset categories is a result of purchases being less than anticipated due to supply chain delays.

Liabilities

Total liabilities are \$17.126 million lower (2%) than original budget. The variance is largely attributable to the employee provision being less than budget due to the impact of movements in the 10 year bond rate.

Statement of changes in equity

Total equity is \$46.039 million higher than budget. The result reflects the \$20.811 million additional surplus against original budget from continuing operations and a \$31.023 million variance in the opening balance on retained earnings. Opening balances in the original budget include estimated actuals at the time the 2021–22 PBS was developed prior to the end of the 2020–21 financial year. Additionally \$5.791 million of departmental capital budget has been quarantined by the Department of Finance as an approved movement of funds request with the amount to be reappropriated after the appropriations extinguishment period (due to the three-year sun setting clause).

Statement of cash flows

The amounts reported in the statement of cash flows reflect the cash impact of 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.





APPENDICES

Appendix A: ASIO resource statement

	Actual available appropriation 2022 \$'000	Payments made 2022 \$'000	Balance remaining 2022 \$'000
Departmental			
Annual appropriations—ordinary annual services ¹			
Prior year appropriation	125 696	125 696	-
Departmental appropriation ²	480 266	382 700	97 566
Section 74 external revenue ³	35 132	31 358	3774
Departmental capital budget ⁴	38 488	14 820	23 668
Cash on hand	13 787	(8469)	22 256
Annual appropriations—other services—non-operating ⁵			
Prior year appropriation	7919	7919	-
Equity injections	48 501	30 501	18 000
Total net resourcing and payments for ASIO	749 789	584 525	165 264

¹ Appropriation Act (No.1) and Appropriation Act (No. 3).

² Excludes departmental capital budget (DCB).

³ External receipts under section 74 of the *Public Governance, Performance and Accountability Act 2013*.

⁴ Departmental capital budgets are not separately identified in 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'.

⁵ Supply Act (No.2), Appropriation Act (No.2) and 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 ¹ 2022 \$'000	Actual expenses 2022 \$'000	Variation 2022 \$'000
Program 1.1: Security Intelligence			
Departmental expenses			
Departmental appropriation	480 266	420 686	59 580
Section 74 external revenue ²	24 579	35 132	(10 553)
Expenses not requiring appropriation in the budget year ³	115 056	140 868	(25 812)
Total for Program 1.1	619 901	596 686	23 215
Total expenses for Outcome 1	619 901	596 686	23 215

¹ Full-year budget, including any subsequent adjustments made at Additional Estimates and reductions under *Public Governance, Performance and Accountability Act 2013* section 51.

² Expenses incurred in relation to receipts retained under *Public Governance, Performance and Accountability Act 2013* section 74.

³ Expenses not requiring appropriation in the budget year are depreciation, amortisation expenses and resources received free of charge.

Appendix C: report of the Independent Reviewer of Adverse Security Assessments

Appointment of the Independent Reviewer of Adverse Security Assessments

Mr Robert Cornall AO was first appointed as Independent Reviewer of Adverse Security Assessments on 4 September 2015. He completed his appointment on 16 January 2022 and Mr Philip Moss AM was appointed Independent Reviewer for a term of three years commencing on 17 January 2022.

The role of the Independent Reviewer

The Independent Reviewer of Adverse Security Assessments conducts an independent advisory review of any Australian Security Intelligence Organisation (ASIO) adverse security assessment (ASA) furnished to the Department of Home Affairs in respect of an eligible person, being such a person who:

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

The Independent Reviewer's terms of reference and other relevant information are available at www.ag.gov.au/asareview.

The Independent Reviewer undertakes a primary review of each adverse security assessment which comes within the terms of reference and 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.

In the past, the Independent Reviewer has commonly delayed a periodic review pending the outcome of an internal review by ASIO with the agreement of the person's solicitor. This arrangement has avoided the need for the person to respond to two reviews about the same matter at the same time.

It also recognises the reality that:

- if the internal review results in a qualified or non-prejudicial security assessment, the person no longer falls within the Reviewer's terms of reference and no periodic review is required, or
- if the internal review results in a further adverse security assessment, that ASA will become the subject of a primary review, replacing the former ASA and the need for the outstanding periodic review.

I have decided to adopt this approach in relation to annual periodic reviews and have informed relevant legal representatives accordingly.

Reviews required or undertaken during the year

During the year, the Independent Reviewer dealt with adverse security assessments furnished in respect of four eligible persons. Of these four cases, two were dealt with and finalised during the reporting year and two remain current.

Case 1 (being Person 3 in the Independent Reviewer's 2020–21 Report): At the commencement of the year, ASIO was undertaking an internal review of this person's adverse security assessment furnished on 16 October 2019.

On 20 August 2021, ASIO advised the Reviewer:

... that on 17 August 2021 the Director-General of Security approved furnishing a non-prejudicial security assessment to the Department of Home Affairs in respect of [the person's] suitability to hold a permanent protection visa.

This outcome was the first time an internal review had resulted in a non-prejudicial security assessment during the former Independent Reviewer's six-year period in office. ASIO advised the change of circumstances that had led to this outcome in an email dated 1 December 2021:

The change in circumstances giving rise to a new assessment for [the person] included new information provided by [the person], the limited new or current adverse reporting about [the person's] activities or associations, and the continued suppression of the people smuggling environment.

As a result, this matter is now at an end.

Case 2 (being Person 5 in the Independent Reviewer's 2020–21 Report): At the commencement of the year, ASIO was also undertaking an internal review of this person's adverse security assessment furnished on 20 November 2017.

Before the internal review was completed, ASIO advised in an email dated 30 November 2021 that:

On 23 November ASIO received information from Home Affairs that [the person] had elected to be voluntarily removed from Australia and is due to depart on 13 December 2021. ... in the light of the above information we will no longer be progressing this review.

The Independent Reviewer was subsequently advised on 20 December 2021 that [the person] had departed Australia.

The Independent Reviewer informed the person's solicitor of these communications and that this matter was now at an end.

Case 3 (being Person 2 in the Independent Reviewer's 2020–21 Report): Person 2 was the subject of an adverse security assessment dated 21 October 2019 which was replaced by a second ASA furnished to Home Affairs on 15 July 2020.

The former Independent Reviewer provided a primary review of the second ASA on 15 March 2021. The Independent Reviewer concluded:

Based on all the information before this review, it is my view that [the person] is unlikely to present a direct or indirect risk to security in future. In accordance with the opinion expressed above and the provisions of the ASIO Act, my recommendation is that ASIO issue a qualified security assessment in respect of [the person].

The Director-General did not accept this advisory recommendation. The ASA remained on foot and due for a periodic review commencing in March 2022.

On 9 May 2022, the Director-General informed me that ASIO had commenced an internal review of the person's adverse assessment. This internal review is expected to be completed by August 2022. In the meantime, this person (now re-named Person A for the purposes of this report), who was detained in 2019, remained in immigration detention.

If this internal review results in a new ASA, I will conduct a primary review during the 2022–23 financial year. If the outcome is a qualified or non-prejudicial security assessment, my function as the Independent Reviewer would cease in relation to Person A.

Case 4 (being Person 4 in the Independent Reviewer's 2020–21 Report): Person 4 (now renamed Person B for the purposes of this report) has been the subject of two adverse security assessments which have been reviewed by the Independent Reviewer. The second ASA was furnished by ASIO on 27 October 2020 and the Independent Reviewer's primary review was delivered on 5 May 2021.

At the commencement of the year, the second ASA remained on foot and due for a periodic review by the Independent Reviewer in May 2022. On 31 May 2022, the Director-General wrote to me as follows.

As you know, the Federal Court of Australia [Plaintiff S111A/2018 v Minister for Home Affairs (No 4) [2022] FCA 329] made final orders setting aside Adverse Security Assessments (ASAs) furnished in 2018 and 2020 in respect of [the person] and Minister for Home Affairs' decision to refuse [the person] a protection visa. I have approved filing an appeal of the orders setting aside the ASAs.

Because the Minister's decision to refuse [the person] a protection visa has been set aside, a new visa decision will need to be made by the Minister. I can advise ASIO has commenced a new security assessment for the visa decision process following referral from the Department of Home Affairs.

In the meantime, Person B remains in immigration detention. If the new security assessment were to result in an ASA, I would commence a primary review. Person B has been held in immigration detention since 2012.

New matters arising during the year

There were no new matters referred to the Independent Reviewer during 2021–22.

Post 30 June 2022 development

On 5 August 2022, the Director-General furnished a non-prejudicial security assessment to the Department of Home Affairs in regard to Person A.

Acknowledgement of Mr Robert Cornall AO

The first six and a half months of the period covered by this report relate to Mr Cornall's term of appointment as Independent Reviewer. I take this opportunity to acknowledge Mr Cornall's longstanding contribution in the role and to thank him for his work during that time and support when I commenced.

Philip Moss AM

Independent Reviewer of Adverse Security Assessments

Appendix D: executive remuneration

Key management personnel remuneration

Categories of ASIO's key management personnel include:

- the Director-General of Security; and
- members of the Executive Committee.

The following tables show the remuneration of key management personnel, senior executives and other highly paid staff in 2021–22 in accordance with the *Public Governance, Performance and Accountability Rule 2014*.

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.

Information about remuneration for key management personnel

Name	Term	Position title	Short-term benefits			Post-employment benefits			Termination benefits		Total remuneration
			Base salary ¹	Bonuses	Other benefits and allowances	Superannuation contributions	Long service leave ²	Other long-term benefits	benefits	benefits	
			\$	\$	\$	\$	\$	\$	\$	\$	\$
Mike BURGESS	1 Jul 21– 30 Jun 22	Director-General ³	631 972	0	0	89 409	14 494	0	0	0	735 875
Heather COOK	1 Jul 21– 18 Mar 22	Deputy Director-General	249 189	0	0	48 551	26 644	0	0	0	324 383
Chris TEAL	19 Mar 22– 30 Jun 22	Deputy Director-General	112 712	0	0	19 132	3705	0	0	0	135 548
Hazel BENNETT	1 Jul 21– 30 Jun 22	Deputy Director-General	493 795	0	0	80 402	13 329	0	0	0	587 526
Ewan MACMILLAN	16 May 22– 30 Jun 22	Deputy Director-General	51 855	0	0	9 370	39 008	0	0	0	100 232
Name withheld ⁴	1 Jul 21– 30 Jun 22	Principal Advisor	359 584	0	0	58 277	10 559	0	0	0	428 421
Name withheld ⁴	1 Jul 21– 3 Apr 22	General Counsel	273 328	0	0	46 077	6084	0	0	0	325 488
Name withheld ⁴	4 Apr 22– 30 Jun 22	General Counsel	84 892	0	0	11 765	3264	0	0	0	99 921

¹ 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*.

² Does not represent one year's leave accrual at officer's current salary. Value is in accordance with Department of Finance requirements; *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*.

³ The prorata remuneration in this table differs from that shown in *Remuneration Tribunal (Remuneration and Allowances for Holders of Full-time Public Office) Determination 2021* because the Department of Finance (in *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*) specifies a different basis of determining the value of superannuation.

⁴ The Principal Advisor and General Counsel are non-declared officers. To comply with section 92 of the ASIO Act these names have been withheld.

Information about remuneration for senior executives

Remuneration bands	Number of senior executives ¹	Short-term benefits			Post-employment benefits		Other long-term benefits		Termination benefits		Total remuneration
		Average base salary ²	Average bonuses	Average other benefits and allowances	Average superannuation contributions	Average long service leave ³	Average other long-term benefits	Average termination benefits			
		\$	\$	\$	\$	\$	\$	\$	\$	\$	
\$0 to \$220 000	12	65 775	0	0	9869	3218	0	0	0	0	78 863
\$220 001 to \$245 000	2	191 031	0	0	29 185	10 996	0	0	0	0	231 212
\$270 001 to \$295 000	2	236 612	0	0	30 463	22 226	0	0	0	0	289 301
\$295 001 to \$320 000	24	250 601	0	3826	42 352	8417	0	0	0	0	305 196
\$320 001 to \$345 000	6	273 075	0	2011	40 007	15 189	0	0	0	0	330 282
\$345 001 to \$370 000	3	274 262	0	14 867	42 827	25 601	0	0	0	0	357 557
\$370 001 to \$395 000	6	310 913	0	6381	50 472	10 171	0	0	0	0	377 936
\$395 001 to \$420 000	3	320 415	0	13 801	45 722	16 943	0	0	0	0	396 882
\$445 001 to \$470 000	1	385 380	0	0	56 732	4351	0	0	0	0	446 463
\$495 001 to \$520 000	2	350 513	0	7325	43 415	7045	0	0	95 342	0	503 640

¹ Several senior executive positions were occupied by different officers for portions of the year.

² 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*.

³ Does not represent one year's leave accrual at officer's current salary. Value is in accordance with Department of Finance requirements: *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*.

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 ¹	Average bonuses	Average other benefits and allowances	Average superannuation contributions	Average long service leave ²	Average other long-term benefits	Average termination benefits			
		\$	\$	\$	\$	\$	\$	\$	\$	\$	
\$220 001 to \$245 000	16	196 664	0	5050	27 949	9218	0	0	0	238 880	
\$245 001 to \$270 000	18	211 868	0	1400	35 087	8893	0	0	0	257 248	
\$270 001 to \$295 000	7	240 691	0	3157	30 027	7612	0	0	0	281 488	
\$295 001 to \$320 000	2	238 844	0	32 969	29 631	6430	0	0	0	307 873	
\$320 001 to \$345 000	6	259 747	0	1091	24 596	16 482	0	34 484	0	336 400	
\$345 001 to \$370 000	2	312 554	0	0	30 134	6681	0	0	0	349 369	
\$470 001 to \$495 000	2	314 639	0	0	38 117	9513	0	114 765	0	477 034	

¹ 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*.

² Does not represent one year's leave accrual at officer's current salary. Value is in accordance with Department of Finance requirements: *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*.

Appendix E: ASIO's salary classification structure

Senior Executive Service	Minimum salary	Maximum salary
SES Band 3	\$332 943	
SES Band 2	\$259 047	
SES Band 1	\$207 237	

Senior employees		
AEE3	\$166 399	
AEE2	\$140 621	\$166 399
AEE1	\$122 690	\$137 106

Employees		
AE6	\$96 535	\$108 769
AE5	\$87 344	\$93 751
AE4	\$79 593	\$85 398
AE3	\$70 391	\$76 916
AE2	\$61 909	\$68 574
AE1	\$53 438	\$59 362

Note: Figures are as applied in 2021–22 and exclude Individual Salary Agreements. 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 at ASIO.

Appendix F: workforce statistics by headcount

Public Governance, Performance and Accountability Rule (PGPA Rule) section 17AG(4)(aa)

Statistics of ongoing employees by gender—current report period (2021–22)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
Total	897	41	938	678	213	891	-	-	-	1829

PGPA Rule section 17AG(4)(aa)

Statistics of non-ongoing employees by gender—current report period (2021–22)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
Total	2	13	15	-	3	3	-	-	-	18

PGPA Rule section 17AG(4)(aa)

Statistics of ongoing employees by gender—previous report period (2020–21)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
Total	964	40	1004	686	231	917	-	-	-	1921

PGPA Rule section 17AG(4)(aa)

Statistics of non-ongoing employees by gender—previous report period (2020–21)

	Male			Female			Indeterminate			Total
	Full-time	Part-time	Total male	Full-time	Part-time	Total female	Full-time	Part-time	Total indeterminate	
Total	3	10	13	2	4	6	-	-	-	19

PGPA Rule section 17AG(4)(aa)

Statistics on full-time and part-time employees—current report period (2021–22)

	Ongoing			Non-ongoing			Total
	Full-time	Part-time	Total ongoing	Full-time	Part-time	Total non-ongoing	
Total	1575	254	1829	2	16	18	1847

PGPA Rule section 17AG(4)(aa)

Statistics on full-time and part-time employees—previous report period (2020–21)

	Ongoing			Non-ongoing			Total
	Full-time	Part-time	Total ongoing	Full-time	Part-time	Total non-ongoing	
Total	1650	271	1921	5	14	19	1940

PGPA Rule section 17AG(4)(aa)

Employment type by location—current report period (2021–22)¹

	Ongoing	Non-ongoing	Total
All locations	1829	18	1847
Total	1829	18	1847

PGPA Rule section 17AG(4)(aa)

Employment type by location—previous report period (2020–21)²

	Ongoing	Non-ongoing	Total
All locations	1921	19	1940
Total	1921	19	1940

¹ Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, the locations of staff has been deleted from the version of the Annual Report 2021–22 tabled in Parliament. (Appendix S)

² Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, the locations of staff has been deleted from the version of the Annual Report 2021–22 tabled in Parliament. (Appendix S)

PGPA Rule section 17AH(1)(c)

People with a disability employment—current reporting period (2021–22)

	Total
Ongoing	25
Non-ongoing	-
Total	25

PGPA Rule section 17AH(1)(c)

People with a disability employment—previous reporting period (2020–21)

	Total
Ongoing	27
Non-ongoing	-
Total	27

Appendix G: recruitment, advertising and market research

ASIO seeks exceptional people for exceptional careers. We seek to reflect the diversity of the community we protect, and continue to develop and implement attraction strategies to achieve this.

In the financial year 2021–22, ASIO expended \$626 761 on advertising and marketing for recruitment activities and campaigns. Further information on these advertising campaigns is available at 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.

During the reporting year, ASIO continued to adapt and refine its approach to recruitment in response to the evolving COVID-19 environment. There was a greater focus on growing our own capability through entry-level roles in intelligence, technology and corporate functions, and technologist recruitment more broadly.

ASIO is endeavouring to increase awareness in the community of ASIO careers through its presence on social media platforms.

Appendix H: work health and safety

ASIO is committed to providing a safe work environment for all staff. Work health and safety considerations are integrated into the planning and delivery of ASIO's activities across a range of work environments.

ASIO has initiated a number of programs aimed at building a positive safety culture, promoting health and wellbeing, and increasing safety awareness within the workforce.

Our safety risk management strategies reinforce legislative compliance and a culture of continual improvement, focused on identifying and monitoring safety risks and implementing appropriate controls.

ASIO is actively engaged with the challenges of COVID-19 and, in response to the pandemic, the Organisation has implemented a range of strategies to manage risks to ASIO's core business functions and to the safety of its workforce.

Health and wellbeing

ASIO's health and wellbeing program aims to promote positive physical and psychological wellbeing by encouraging staff to take proactive steps in relation to their wellbeing.

The current program includes varied wellbeing initiatives such as the:

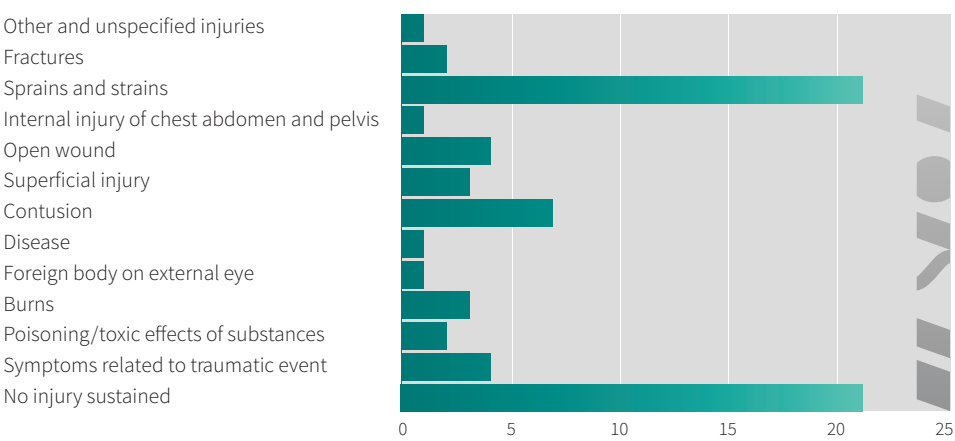
- workplace influenza vaccination program;
- Employee Assistance Program and Manager Assist service;
- ergonomic program; and
- health promotion—including Work Health and Safety Month, RuOK? Day and Mental Health Week.

Incidents

In accordance with legislated notification obligations, ASIO reported two incidents to Comcare in 2021–22. Comcare was provided with detailed information about the incidents and the process that ASIO was undertaking to address the incidents. In response to the reports, no further action was taken by Comcare.

The following table outlines safety incidents by mechanism of injury for the period 2021–2022.

Table 5: Total number of injuries by type



Appendix I: ecologically sustainable development and environmental performance

ASIO is committed to enhancing our environmental sustainability. We strive to operate in an environmentally responsible manner, making every effort to use our resources efficiently and manage our waste effectively.

Theme	Performance measure	Indicator(s) ¹	2020–21	2021–22
Energy efficiency	Total consumption of energy	Amount of electricity consumed (kWh)	20 103 439	20 448 315
		Amount of gas consumed (MJ)	15 146 638	12 620 048
		Amount of other fuels consumed (L)	68 306	50 191
	Total production of energy from sources other than grid-connected electricity provider	Total amount of energy produced (kWh) from alternate sources	443 834	231 698
		Energy produced (kWh) from gas cogeneration plant	180 072	35 258
		Energy produced (kWh) from solar panels (green energy)	263 762	196 440
	Greenhouse gas emissions	Amount of greenhouse gases produced (tonnes)	23 886	15 227
	Environmental Performance targets—tenant light & power (TL&P) and central services	TL&P less than 7,500 MJ/person/annum	11 956	10 255
		Central services less than 400 MJ/m ² /annum	575	360
	Energy rating	NABERS ² Energy for Offices (1-6)	6 stars	6 stars

Theme	Performance measure	Indicator(s) ¹	2020–21	2021–22
	Steps taken to reduce effect	Measures to review and improve reducing the effect		
	Work continued on the LED light replacement program to reduce the use of fluorescent and metal-halide lights	ASIO again participated in national environmental events such as Earth Hour		
	Optimising the efficiency of the air-conditioning system—reducing the demand on boilers, chillers and cooling towers			
	Regular scheduled cleaning of solar panels to maximise energy production			
Waste³	Total waste production—this includes all waste (unwanted by-products) produced when undertaking the functions of the agency	Amount of waste produced (tonnes)	180.85	123.75
	Un-recyclable waste production—this includes all wastes that are not re-used or recycled	Amount of waste going to landfills (tonnes)	46.50	35.07
	Recyclable waste production (excluding office paper)	Amount of waste going to recycling facilities (tonnes)	126.46	76.51
	Paper usage	Amount of waste paper going to recycling facilities (tonnes)	7.89	12.17
		Amount of paper sourced from recyclable sources (tonnes)	10.81	10.04
		Percentage of paper sourced from recyclable sources	100	96
	Relative waste production	Amount of the total waste (kg) per employee	126.91	83.84
	Waste rating	NABERS waste rating (1–6)	6 stars	5 stars

Theme	Performance measure	Indicator(s) ¹	2020–21	2021–22
	Steps taken to reduce effect	Measures to review and improve reducing the effect		
	‘Follow-me’ printing and double sided printing and copying remained as the default setting on printers to reduce paper waste	Refining waste processes and minimisation techniques		
	Continued sourcing office copy paper from sustainably managed sources	Continue to promote environmental awareness across our organisation through sustainable initiatives		
	Used coffee bean grounds continue to be mulched into the garden beds of the Ben Chifley Building			
Water	Total consumption of water—this includes all water consumed when undertaking the functions of the agency	Amount of water consumed (kL)	48 245	47 695
	Rainwater capture and use—includes all rainwater captured on site	Amount of rainwater captured (ML)	15.33	18.33
		Amount of captured rainwater used (ML)	15.33	18.33
	Relative consumption of water—per employee	Amount of total water use (kL) per employee	33.86	32.31
	Water rating	NABERS water rating (1–6)	1.5 stars	2.5 stars
	Steps taken to reduce effect	Measures to review and improve reducing the effect		
	ASIO consumes fresh water from the public water network, artesian water sources and rainfall	All captured stormwater is used, for irrigation and toilet flushing—reducing the reliance on potable and bore water		

Notes:

- Figures relate to ASIO's Ben Chifley Building only.
- 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.
- Waste data is supplied by an external contractor. Where accuracy is impacted by circumstances out of ASIO's control, a correction based on the known monthly weight collections has been applied.

Appendix J: report on use of questioning warrants

ASIO is required under section 94 of the ASIO Act to provide in its annual report details of its use of questioning warrants.

Item 18 of Schedule 1 to the *Australian Security Intelligence Organisation Amendment Act 2020* (ASIO Amendment Act) provides that section 94 of the ASIO Act as amended by Part 1 of Schedule 1 to the ASIO Amendment Act applies in relation to annual reports prepared on or after the commencement of item 18.

The details are provided in the following table.

Subsection	Description	2019–20	2020–21	2021–22
94(1)(a)	The total number of requests made during the period under Division 3 of Part III to the Attorney-General for the issue of warrants under that Division (including the number of requests made orally)	0	3	1
94(1)(b)	The total number of warrants issued during the period under that Division (including the number of warrants issued orally)	0	3	1
94(1)(c)	The number of times persons were apprehended during the period under that Division	0	0	0
94(1)(d)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the period under that Division and the total of all those hours for all those persons	-	see below	see below
	Person 1		7 hours, 33 minutes*	
	Person 2		6 hours, 40 minutes*	
	Person 3	-	-	4 hours, 43 minutes*
	Total hours		14 hours, 13 minutes	4 hours, 43 minutes
94(1)(e)	The number of times each prescribed authority had persons appear for questioning before the prescribed authority under warrants issued during this reporting period under that Division	-	see below	see below
	Prescribed authority 1	0	2	0
	Prescribed authority 2	0	0	1

* These hours are a cumulative total of multiple questioning periods for each person

Appendix K: correction of material errors in previous annual report

This appendix provides correction of material errors in the previous annual report which have proved to be wrong, in accordance with paragraph 17AH(1)(e) of the *Public Governance, Performance and Accountability Rule 2014*.

The following are corrections to reporting errors made in the *ASIO Annual Report 2020–21*.

On page 18 in the graphic titled ‘Disruptions and attacks 2014–21’, it was incorrectly listed that there were six Sunni violent extremism disruptions in the year for 2016. The correct number of Sunni violent extremism disruptions for 2016 is five.

On page 37 in Chapter 4 ‘Report on performance’ under the heading ‘Our advice was relevant and practical’, the date provided for both examples is August 2020. The correct date for these examples is July 2020. Similarly, under the heading ‘Our advice influenced decision-making’, the date of February 2021 should read December 2020. These errors did not detract from the substance of the content describing the activities undertaken by ASIO.

On page 77 in Chapter 5 ‘Management and accountability’, information contained under the heading ‘Administrative Appeals Tribunals’ and ‘Tribunal reviews—archives matters’ incorrectly recorded that three matters related to reviews of National Archives access decisions involving ASIO material. The correct number of matters related to reviews of National Archives access decisions involving ASIO material is four.

On page 108 in Financial statements under the heading ‘2. Financial position’ the table heading incorrectly lists the reporting years as 2020 and 2019. The correct years for this table are 2021 and 2020. This error does not impact the reported expenditure figures which remain accurate for 2021 and 2020 dates.

On page 122 in Financial statements under the heading ‘Assets’ the first sentence incorrectly notes that the total assets are 5% lower than original budget. The correct figure should read 2% lower than original budget. This error does not impact the reported asset figure of \$20.391 million which is correctly recorded.

On page 133 in ‘Appendix D: ASIO’s salary classification structure’ in the table ‘Employment salary ranges by classification level’ the maximum salary for SES Band 2 is incorrectly recorded as \$279 500. The correct figure should be \$301 000.

On page 136 in ‘Appendix E: workforce statistics by headcount’, the total numbers provided for the tables ‘Employees by full-time and part-time employment status—current reporting period (2020–21)’ and ‘Employees by full-time and part-time employment status—previous reporting period (2019–20)’ are incorrect and do not accurately reflect ASIO staffing figures for those time periods. The corrected tables are provided in the following table.

Employees by full-time and part-time employment status—current reporting period (2020–21)

	Ongoing			Non-ongoing			Total
	Full-time	Part-time	Total ongoing	Full-time	Part-time	Total non-ongoing	
SES 3	3	0	3	0	0	0	3
SES 2	10	0	10	0	0	0	10
SES 1	37	0	37	0	0	0	37
AEE1–3	551	86	637	0	4	4	641
AE1–6	1049	185	1234	5	10	15	1249
Total	1650	271	1921	5	14	19	1940

Employees by full-time and part-time employment status—previous reporting period (2019–20)

	Ongoing			Non-ongoing			Total
	Full-time	Part-time	Total ongoing	Full-time	Part-time	Total non-ongoing	
SES 3	3	0	3	0	0	0	3
SES 2	15	0	15	0	0	0	15
SES 1	44	0	44	0	0	0	44
AEE1–3	557	99	656	2	6	8	664
AE1–6	1077	185	1262	6	10	16	1278
Total	1696	284	1980	8	16	24	2004

In Appendix M, one statistic required under section 94(2A)(c) of the ASIO Act was omitted. As a result, statistics required under section 94(2A)(d) were incorrect. Corrected figures are included in Appendix M to the *ASIO Annual Report 2021–22*.

On pages 142 to 144 in ‘Appendix H: ecologically sustainable development and environmental performance’, some of the energy efficiency and waste numbers reported were incorrect. The corrected entries are provided in the following table.

Theme	Performance measure	Indicator(s)	Reported number	Corrected number
Energy efficiency	Total consumption of energy	Amount of gas consumed (MJ)	14 149 220	15 146 638
		Amount of other fuels consumed (L)	101 197 (diesel)	68 306 (diesel & petrol)
	Energy rating	NABERS ¹ Energy for Offices (1-6)	3.5 stars	6 stars
	Total waste production—this includes all waste (unwanted by-products) produced when undertaking the functions of the agency	Amount of waste produced (tonnes)	194.98	180.85
	Un-recyclable waste production—this includes all wastes that are not re-used or recycled	Amount of waste going to landfills (tonnes)	57.59	46.50
	Recyclable waste production (excluding office paper)	Amount of waste going to recycling facilities (tonnes)	137.39	126.46
Waste	Paper usage	Amount of waste paper going to recycling facilities (tonnes)	8.40	7.89
	Un-recyclable waste production—this includes all wastes that are not re-used or recycled	Amount of paper sourced from recyclable sources (tonnes)	1.30	10.81
	Recyclable waste production (excluding office paper)	Percentage of paper sourced from recyclable sources	20	100
	Relative waste production	Amount of the total waste (kg) per employee	87.05	126.91
	Waste rating	NABERS Waste Rating (1-6)	3 stars	6 stars

Material errors previously corrected

On page 149 in Appendix J, figures provided under section 94(1)(d) of the ASIO Act were reported incorrectly.

On identifying the error, ASIO tabled a correction in Parliament on 24 November 2021, following which the *ASIO Annual Report 2020–21* was updated to reflect the correct figures.

In Appendix O, statistics required under section 94(2BD) of the ASIO Act were omitted. On identifying the error, ASIO provided advice to the Minister for Home Affairs on 18 November 2021, correcting this omission in an amended Appendix O. Appendix O was also provided to the Leader of the Opposition as per section 94 of the ASIO Act.

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 PGPA Rule. Section 17AJ(d) requires this table be included in entities' annual reports as an aid of access.

PGPA Rule reference	Description	Requirement	Part of this report
17AD(g)	Letter of transmittal		
17AI	A copy of the letter of transmittal signed and dated by accountable authority on date final text approved, with 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
17AD(h)	Aids to access		
17AJ(a)	Table of contents (print only).	Mandatory	Preliminaries
17AJ(b)	Alphabetical index (print only).	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
17AD(a)	Review by an accountable authority		
17AD(a)	A review by the accountable authority of the entity.	Mandatory	Part 1
17AD(b)	Overview of the entity		
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 and Part 4
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 2
17AE(1)(aa)(ii)	Position title of the accountable authority or each member of the accountable authority.	Mandatory	Part 2
17AE(1)(aa)(iii)	Period as the accountable authority or member of the accountable authority within the reporting period.	Mandatory	Part 2
17AE(1)(b)	An outline of the structure of the portfolio of the entity.	Portfolio departments mandatory	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.	Mandatory (if applicable)	Not applicable
17AD(c)	Report on the performance of the entity		
	<i>Annual performance statements</i>		
17AD(c)(i); 16F	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule.	Mandatory	Part 4
17AD(c)(ii)	<i>Report on Financial Performance</i>		
17AF(1)(a)	A discussion and analysis of the entity's financial performance.	Mandatory	Part 4 Part 6 and Appendix Q
17AF(1)(b)	A table summarising the 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.	Mandatory (if applicable)	Not applicable

PGPA Rule reference	Description	Requirement	Part of this report
17AD(d)	Management and accountability		
	<i>Corporate governance</i>		
17AG(2)(a)	Information on compliance with section 10 (fraud systems).	Mandatory	Letter of transmittal and Part 5
17AG(2)(b)(i)	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	Letter of transmittal
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 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.	Mandatory (if applicable)	Not applicable
	<i>Audit Committee</i>		
17AG(2A)(a)	A direct electronic address of the charter determining the functions of the entity's audit committee.	Mandatory	Appendix R
17AG(2A)(b)	The name of each member of the entity's audit committee.	Mandatory	Appendix R
17AG(2A)(c)	The qualifications, knowledge, skills or experience of each member of the entity's audit committee.	Mandatory	Appendix R
17AG(2A)(d)	Information about the attendance of each member of the entity's audit committee at committee meetings.	Mandatory	Appendix R
17AG(2A)(e)	The remuneration of each member of the entity's audit committee.	Mandatory	Appendix R
	<i>External scrutiny</i>		
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.	Mandatory (if applicable)	Part 5

PGPA Rule reference	Description	Requirement	Part of this report
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.	Mandatory (if applicable)	Part 5
17AG(3)(c)	Information on any capability reviews on the entity that were released during the period.	Mandatory (if applicable)	Part 4 and Part 5
Management of human resources			
17AG(4)(a)	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	Part 5
17AG(4)(aa)	Statistics on the entity's employees on an ongoing and non-ongoing basis, including the following: a. statistics on full-time employees; b. statistics on part-time employees; c. statistics on gender; and d. statistics on staff location.	Mandatory	Appendix F Appendix S
17AG(4)(b)	Statistics on the entity's Australian Public Service (APS) employees on an ongoing and non-ongoing basis; including the following: ■ Statistics on staffing classification level; ■ Statistics on full time employees; ■ Statistics on part time employees; ■ Statistics on gender; ■ Statistics on staff location; ■ Statistics on employees who identify as Indigenous.	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	Not applicable
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	Not applicable
17AG(4)(c)(ii)	The salary ranges available for APS employees by classification level.	Mandatory	Appendix E
17AG(4)(c)(iii)	A description of non salary benefits provided to employees.	Mandatory	Part 5
17AG(4)(d)(i)	Information on the number of employees at each classification level who received performance pay.	Mandatory (if applicable)	Not applicable
17AG(4)(d)(ii)	Information on aggregate amounts of performance pay at each classification level.	Mandatory (if applicable)	Not applicable

PGPA Rule reference	Information on aggregate amounts of performance pay at each classification level	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.	Mandatory (if applicable)	Not applicable
17AG(4)(d)(iv)	Information on aggregate amount of performance payments.	Mandatory (if applicable)	Not applicable
Assets management			
17AG(5)	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	Mandatory (if applicable)	Part 5
Purchasing			
17AG(6)	An assessment of entity performance against the <i>Commonwealth Procurement Rules</i> .	Mandatory	Part 5
Reportable consultancy contracts			
17AG(7)(a)	A summary statement detailing the number of new reportable consultancy contracts entered into during the period; the total actual expenditure on all such contracts (inclusive of GST); the number of ongoing reportable consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST).	Mandatory	Part 5
17AG(7)(b)	A statement that <i>"During [reporting period], [specified number] new reportable consultancy contracts were entered into involving total actual expenditure of \$[specified million]. In addition, [specified number] ongoing reportable 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 reportable consultancy contracts. Information on the value of reportable consultancy contracts is available on the AusTender website."</i>	Mandatory	Part 5

PGPA Rule reference	Description	Requirement	Part of this report
Reportable non-consultancy contracts			
17AG(7A)(a)	A summary statement detailing the number of new reportable non-consultancy contracts entered into during the period; the total actual expenditure on such contracts (inclusive of GST); the number of ongoing reportable non-consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST).	Mandatory	Part 5
17AG(7A)(b)	A statement that <i>"Annual reports contain information about actual expenditure on reportable non-consultancy contracts. Information on the value of reportable non-consultancy contracts is available on the AusTender website."</i>	Mandatory	Part 5
17AD(daa) Additional information about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts			
17AGA	Additional information, in accordance with section 17AGA, about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts.	Mandatory	Not applicable
Australian National Audit Office access clauses			
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.	Mandatory (if applicable)	Not applicable
Exempt contracts			
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 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.	Mandatory (if applicable)	Not applicable
Small business			
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

PGPA Rule reference	Description	Requirement	Part of this report
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 “[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 the Treasury’s website.”	Mandatory (if applicable)	Part 5
Financial statements			
17AD(e)	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	Part 6 and Appendix Q
Executive remuneration			
17AD(da)	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 2–3 of the Rule.	Mandatory	Appendix D
17AD(f) Other mandatory information			
17AH(1)(a)(i)	<i>If the entity conducted advertising campaigns, a statement that “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>	Mandatory (if applicable)	Part 5
17AH(1)(a)(ii)	If the entity did not conduct advertising campaigns, a statement to that effect.	Mandatory (if applicable)	Not applicable
17AH(1)(b)	<i>A statement that “Information on grants awarded by [name of entity] during [reporting period] is available at [address of entity’s website].”</i>	Mandatory (if applicable)	Not applicable
17AH(1)(c)	Outline of mechanisms of disability reporting, including reference to 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 previous annual report.	Mandatory (if applicable)	Appendix K
17AH(2)	Information required by other legislation.	Mandatory	Part 5 and Appendices

Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, the Director-General of Security has made deletions from the annual report tabled in Parliament, including to **Appendix Q**, **Appendix R** and **Appendix S**.

List of annual report requirements under the ASIO Act

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

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

Consistent with section 94(5) of the ASIO Act, the Minister for Home Affairs, on advice from the Director-General of Security, has made deletions from the annual report tabled in Parliament, including to **Appendix L**, **Appendix M**, **Appendix N**, **Appendix O** and **Appendix P**.

Abbreviations and short forms

A

AASB—Australian Accounting Standards Board

AASB 16—Australian Accounting Standards Board Standard ‘Leases’

AAT—Administrative Appeals Tribunal

ACSC—Australian Cyber Security Centre

AE—ASIO employee

AEE—ASIO executive employee

ANAO—Australian National Audit Office

APS—Australian Public Service

Archives Act – Archives Act 1983

ASA—Adverse security assessment

ASIO—Australian Security Intelligence Organisation

ASIO Act—Australian Security Intelligence Organisation Act 1979

ASIO Amendment Act—Australian Security Intelligence Organisation Amendment Act 2020

B

C

CCSF—Commonwealth Child Safe Framework

CCT—COVID-19 Coordination Team

CFITF—Counter Foreign Interference Taskforce

CIC—Capability Investment Committee

CMT—Crisis Management Team

CPR—Commonwealth Procurement Rules

D

E

EFI—Espionage and foreign interference

ESO—Extended Supervision Orders

F

FOI Act—Freedom of Information Act 1982

G

GST—Goods and services tax

H

HRTTO—High Risk Terrorism Offenders

HUMINT—Human intelligence

I

IDP— Internally displaced person

IGIS—Inspector-General of Intelligence and Security

IMVE—Ideologically motivated violent extremism

Independent Reviewer—Independent Reviewer of Adverse Security Assessments

INSLM—Independent National Security Legislation Monitor

ISIL—Islamic State of Iraq and the Levant

J

K

L

M

N

NABERS—National Australian Built Environment Rating System

NIC—National Intelligence Community

NITRO—Notifiable Incidents, Threats and Reportable Observations

NRVE—Nationalist and racist violent extremist

NSSIC—Naval Shipbuilding Sustainment Identity Card

NV—Negative Vetting

O

OSB—Operation Sovereign Borders

P

PBS—Portfolio Budget Statement

PGPA Act—Public Governance, Performance and Accountability Act 2013

PGPA Rule—Public Governance, Performance and Accountability Rule

PJCIS—Parliamentary Joint Committee on Intelligence and Security

PSS—Public Sector Superannuation Scheme

PSSap—Public Sector Superannuation accumulation plan

PV—Positive Vetting

Q

R

RAP—Reconciliation Action Plan

RMVE—Religiously motivated violent extremism

S

SES—Senior Executive Service

SME—Small and medium enterprises

SMMA—Service Management Maturity Assessment

SRO—Senior Responsible Officer

T

TEO—Temporary Exclusion Orders

U

US—United States

V

W

X

Y

Z

Glossary

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

aukus—the trilateral security partnership between Australia, the United Kingdom and the United States

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 capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country

foreign interference—clandestine, deceptive or threatening activity conducted on behalf of a foreign power which aims to affect political or governmental processes or is otherwise detrimental to Australia's interests

foreign power—a foreign government, 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 about individuals, groups or other entities in order to understand known security threats or identify emerging ones

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

radicalisation—the process by which an individual's beliefs move away from a rejection of violence to achieve societal or political change towards an endorsement or promotion of violence to achieve that change

sabotage—damaging or disruptive activity against infrastructure—including electronic systems—to undermine Australia's national security or advantage a foreign power. Acts of sabotage are not limited to irreversible, destructive attacks on physical infrastructure; they can include small-scale, selective and temporary acts of degradation or disruption to networked infrastructure

terrorism—a tactic employed by a group or individual that involves the use of violence to achieve or advance a political, religious or ideological goal

violent extremism—includes ideologically motivated violent extremism which denotes support for violence to achieve political outcomes or in response to specific political or social grievance/s and religiously motivated violent extremism which denotes support for violence to oppose or achieve a specific social, political or legal system based on a religious interpretation

Index

A

Aboriginal and Torres Strait Islander 13, 81
 academia 36
 Administrative Appeals Tribunal (AAT) 78
 Adverse Security Assessments 75, 117, 120, 148
 advertising v, 86, 129, 146
 Africa 22, 46
 al-Qa'ida 22
ASIO Corporate Plan 2021–25 32, 33, 35, 42, 45, 49, 53, 57, 59, 61, 65
ASIO Corporate Plan 2022–26 39
 ASIO Ombudsman 82
 Attorney-General/Attorney-General's Department 42, 45, 135
 Audit and Risk Committee 71, 76, 77, 83
 AUKUS 4, 50, 54
 AusTender 83, 144, 145
 Australian Government Payments to Small Business 146
 Australian National Audit Office (ANAO) 93
Australian Security Intelligence Organisation Act 1979 (ASIO Act) 11, 121
Australia's Disability Strategy 2021–2031 86
 Australia's security environment 19

B

border integrity 11, 31, 33, 56, 57, 59
 border security 12, 31, 35, 36, 57, 59
 budget 32, 37, 62, 67, 82, 97, 98, 99, 100, 106, 110, 111, 115, 116, 136
 Burgess, Mike 7, 12, 14, 29
 business continuity 71, 73

C

Capability and Investment Committee 71, 72
 capability program iv, 12, 30, 31, 34, 35, 37, 38, 60, 61, 62
 clearances 54, 78
 Comcare 130
Commonwealth Child Safe Framework (CCSF) 87, 148
Commonwealth Electoral Act 1918 86
Commonwealth Fraud Control Framework 2017 77
 Commonwealth Procurement Rules (CPR) 83, 84, 148
 communal violence 11, 150
 consultancy contracts 83, 84, 144, 145
 contracts 83, 84, 85, 102, 105, 143, 144, 145
 Corporate governance v, 71, 142
 Counter-espionage and foreign interference 30, 38
 Counter Foreign Interference Taskforce (CFITF) 50, 51, 148
 counter-terrorism 4, 12, 31, 35, 36, 39, 42, 43, 45, 46, 73, 75
 COVID-19 v, 4, 19, 20, 22, 24, 31, 73, 82, 129, 130, 148
 Criminal Code 43, 46, 75
 Crisis Management Team (CMT) 73, 148
 critical infrastructure 5, 51, 54
 crowded places 47
 cyber espionage 21

D

Defence 4, 5, 11, 20, 21, 40, 52

defence industry 5, 21, 52

defence system 11

Department of Finance 84, 85, 86, 111, 122, 123, 124, 129, 145, 146

Department of Foreign Affairs and Trade (DFAT) 42, 45, 46

departmental capital budget 67, 111, 115

Department of Home Affairs iii, 59, 117, 118, 120

depreciation 67, 104, 110, 116

detention 75, 117, 119, 120

diaspora communities 4

Director-General of Security iii, 7, 11, 12, 14, 29, 71, 72, 88, 93, 118, 121, 146, 147

disability 80, 86, 128, 146

disruption 21, 71, 150

Diversity and Inclusion 80

Diversity and Inclusion Strategy 2021–24 80

diversity networks 80

E

electoral integrity 20, 50

electronic systems 21, 85, 150

espionage iv, 4, 5, 11, 12, 19, 21, 30, 31, 33, 35, 36, 38, 39, 40, 48, 49, 50, 51, 52, 53, 54, 73, 150

espionage and foreign interference iv, 12, 19, 30, 31, 33, 35, 36, 38, 39, 40, 48, 49, 50, 52, 53, 54, 73

Executive Committee 71, 72, 76, 108, 109, 121

explosives 23

external scrutiny v, 74, 142

F

Federal and High Court 78

financial statements 67, 77, 82, 93, 95, 101, 146

foreign fighters 45

foreign intelligence 4, 11, 20, 33, 46, 48, 51, 52

foreign intelligence service 51

foreign interference iv, 4, 5, 11, 12, 19, 21, 30, 31, 33, 35, 36, 38, 39, 40, 48, 49, 50, 51, 52, 53, 54, 73, 148, 150

foreign power/s 4, 5, 19, 20, 21, 24, 40, 150

fraud control 77, 142

fraud risk assessment 77, 142

G

gender 81, 126, 143

Goods and Services Tax (GST) 148

governance v, 7, 37, 61, 62, 71, 72, 76, 77, 82, 121, 142

H

High Risk Terrorism Offenders (HRT0) 43, 45, 148

Home Affairs iii, 32, 42, 45, 59, 75, 88, 93, 117, 118, 119, 120, 139, 147

I

ideologically motivated violent extremists/ extremism 4, 22, 23, 33, 41, 46, 150

immigration detention 75, 117, 119, 120

Independent National Security Legislation Monitor (INSLM) 75, 148

Independent Reviewer/Independent Reviewer of Adverse Security Assessments v, 75, 117, 118, 119, 120, 148

Indigenous 80, 81, 143

Indonesia 22

industry 5, 21, 31, 33, 35, 36, 39, 40, 43, 46, 47, 48, 50, 51, 52, 62

Influence and Impact Committee 5, 71, 72
 Inspector-General of Intelligence and Security (IGIS) 74, 75, 148
 Internally Displaced Person (IDP) 44, 148
 international law 75, 117
 Iraq 22, 43, 148
 Islamic State of Iraq and the Levant (ISIL) 22, 148
 Izz al-Din al-Qassam Brigades 46

J

Jemaah Islamiyah 22
 Joint Counter Terrorism Team 43

K

L

Leader of the Opposition 88, 139
 lone actor 3, 4, 23

M

malicious insiders 51, 150
 Middle East 22
 Mike Burgess 7, 12, 14, 29
 Minister for Finance 77, 127, 146
 Minister's Guidelines 75
 minors 23, 43, 86, 87

N

National Australian Built Environment Rating System (NABERS) 133, 134, 138, 149
 National Intelligence Community (NIC) 54, 57, 59, 149
 nationalist and racist violent extremists/ extremism 23
 national security legislation 74

O

organisational structure 14, 140
 Outreach 14, 50, 51, 52
 oversight 15

P

Parliamentary Joint Committee on Intelligence and Security (PJCIS) 46, 74, 83, 84, 149
 people smuggling 31, 33, 56, 57, 59, 118
 people with a disability 128
 performance measures 30, 31, 35, 36, 39
 Portfolio Budget Statement (PBS) 141, 149
 positive vetting 54, 149
 private sector 4, 21
 propaganda 23, 24, 44
 prosecution/s 78
 protection visa 117, 118, 120
 prying minds 5, 52
Public Governance, Performance and Accountability Act 2013 (PGPA Act) 29, 71, 77, 93, 101, 106, 149
 public interest disclosure 82

Q

Quad 4
 questioning warrants v, 88, 135, 147

R

religiously motivated violent extremists/ extremism 22, 44, 150
 risk management 30, 37, 38, 65, 66, 71, 130
 royal commission 7, 74

S

sabotage 5, 21

science and technology 20, 21

Security and Compliance Committee 71, 83

security environment 11, 17, 19, 31, 34, 39, 44, 47, 54, 64

Senate Estimates 7, 74

Senate Legal and Constitutional Affairs Committee 74

Senior Executive Service (SES) employees 125, 149

small and medium enterprises (SME) 84, 85, 145, 149

small business 84, 145

South Asia 22

South-East Asia 22

sovereignty 4, 19, 20, 21

special intelligence operation authorisations/authorities 88, 147

stakeholder survey 42, 57, 59

Sunni violent extremist/extremism 22, 44, 136

Syria 22, 43, 44, 45

T

technical assistance requests 88, 147

telecommunications data 88, 147

Temporary Exclusion Orders 46, 74, 149

terrorism laws 75

terrorist attack 23, 46

transparency 7, 66, 71, 104

U

universities 20

V

vetting 7, 15, 50, 54, 149

violent extremism 4, 22, 23, 33, 41, 44, 46, 136, 148, 149, 150

violent extremists 4, 19, 22, 23

violent protest 4

visa assessments 58

W

warrants v, 88, 135, 147

workforce v, 7, 73, 79, 80, 81, 86, 87, 126, 130, 136

work health and safety v, 130

Work Health and Safety Act 2011 88

Workforce Plan 79

workplace agreement 79

X

Y

Z

zero tolerance 77



asio.gov.au