

Australian Government

Australian Security Intelligence Organisation

ANNUAL REPORT

2024–25

ASIO

Securing Australia—protecting its people

Aids to access

© Commonwealth of Australia 2025

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.

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



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

Use of the Coat of Arms

The Commonwealth Coat of Arms is used in accordance with the December 2014 Commonwealth Coat of Arms: information and guidelines, published by the Department of the Prime Minister and Cabinet and available online (http://pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

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/resources/asio-annual-report-2024-25. The annual report can also be viewed at www.transparency.gov.au.

Contact us

Phone

General inquiries 1800 020 648

Media inquiries 02 6249 8381

Email

media@asio.gov.au

Post

GPO Box 2176, Canberra ACT 2601

Website

www.asio.gov.au

Acknowledgement of Country

The Australian Security Intelligence Organisation acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to all Aboriginal and Torres Strait Islander peoples, their cultures and to their Elders past, present and emerging.



ANNUAL REPORT

2024–25

31 October 2025

Ref: A26372692

The Hon Tony Burke MP
Minister for Home Affairs
Parliament House
Canberra ACT 2600

Dear Minister,

ASIO Annual Report 2024–25

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 2024–25.

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 with advice to remove statements required under subsections 94(2A), 94(2B), 94(2BA), 94(2BBA), 94(2BC) and 94(2BD) 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 17AD(c), 17AD(e), 17AE(1)(a)(ii), 17AG(2A)(a-e), 17AG(4)(aa) and 17AH(1)(c) from the annual report tabled in parliament. These statements are in the classified appendices 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 subparagraphs 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 AM



FOI WARNING: Exempt document under the *Freedom of Information Act 1982*.
Refer related FOI requests to Department of Home Affairs, Canberra

GPO Box 2176 Canberra City ACT 2601

Contents

1 DIRECTOR-GENERAL'S REVIEW 1

Australia's security environment 2

2 OVERVIEW OF ASIO 9

Overview of ASIO 11

Organisational structure 14

Our most important asset is our people 15

3 REPORT ON PERFORMANCE 17

Annual performance statement 2024–25 19

Summary of performance against ASIO's purpose 20

Measuring performance 22

Counter-espionage and foreign interference 24

Counter-terrorism 28

Influence and impact 34

Top Secret–Privileged Access Vetting 38

Report on financial performance 42

4 MANAGEMENT AND ACCOUNTABILITY 45

Corporate governance 47

External scrutiny 49

Compliance 52

Significant legal matters affecting ASIO's business 55

Management of human resources 57

Other mandatory information 62

5 FINANCIAL INFORMATION 69

A APPENDICES 91

Appendix A: ASIO resource statement 93

Appendix B: expenses by outcomes 94

Appendix C: report of the Independent Reviewer of Adverse Security Assessments 95

Appendix D: report of the Independent Reviewer of Security Clearance Decisions 97

Appendix E: executive remuneration 99

Appendix F: ASIO's salary classification structure 103

Appendix G: workforce statistics 104

Appendix H: work health and safety 108

Appendix I: climate statement 110

Appendix J: report on use of questioning warrants 113

Appendix K: correction of material errors in previous annual reports 114

P PRELIMINARIES 117

List of annual report requirements under schedule 2 of the PGPA Rule 119

List of annual report requirements under the ASIO Act 127

Abbreviations and short forms 128

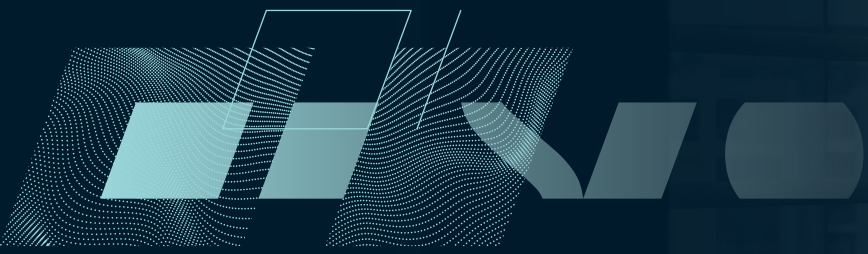
Glossary 130

Index 132





1 DIRECTOR-GENERAL'S REVIEW



Australia's security environment

In 2024–25, Australia entered a period of strategic surprise and security fragility.

A complex, challenging and changing security environment became more dynamic, diverse and degraded.

> "Australia has never faced so many different threats at scale at once, but I am proud of how ASIO has responded to them"



Terrorism

During 2024–25, overseas tensions and conflicts continued to resonate locally, with sentiment amplified by social media and online echo chambers. Conflict in the Middle East did not directly inspire terrorism in Australia, but it did prompt protest, exacerbate division, undermine social cohesion and elevate intolerance. Spikes in politically motivated violence raised the temperature of the security environment and made acts of terrorism more likely.

The national terrorism threat level is currently at **PROBABLE**, and I do not anticipate being able to lower it in the foreseeable future.

While the level of threat is unlikely to change, the form and face of terrorism is evolving. Cases are becoming more complex, with traditional distinctions between extremist motivations breaking down.

During the reporting period, we investigated individuals engaging with religiously motivated violent extremism, and nationalist and racist violent extremist and mixed ideologies. Within the mixed ideologies investigations, we saw people embracing seemingly antithetical concepts, which at times were cherry-picked to create unique, hybrid beliefs. In some cases, individuals adopted violent extremism without a coherent ideology at all.

All of the disrupted terrorist attacks in 2024–25 involved minors or young people, and almost all were lone actors.

Espionage and foreign interference

Extreme levels of espionage and foreign interference did not diminish in 2024–25.

Multiple nations continued their efforts to steal sensitive information, recruit government officials, interfere in our political processes, and monitor, harass, intimidate and coerce cooperation from members of diaspora communities.

Australia's defence capabilities are particularly attractive targets. AUKUS remains a priority for intelligence collection – even by countries considered friendly – and Defence personnel are being targeted both online and in person.

ASIO's response

Australia has never faced so many different threats at scale at once, but I am proud of how ASIO has responded to them.

Response: countering terrorism

ASIO continued to demonstrate its ability to counter terrorist threats, disrupting 4 imminent or advanced onshore plots in 2024–25, in close collaboration with our law enforcement partners.

In one case, ASIO's online operators identified a US-based self-professed neo-Nazi on a popular social networking site. The individual talked about live streaming a school shooting before moving on to a church, synagogue or mosque. ASIO immediately alerted our US counterparts, who were able to prevent a potential massacre – thanks to ASIO intelligence.

Many challenges of the contemporary counter-terrorism environment cannot be solved by ASIO or law enforcement alone.

The impacts of social media, mental health, the spread of misinformation and conspiracy theories, ubiquitous encryption, growing grievance, and the radicalisation of minors all require whole-of-government, whole-of-community, whole-of-society responses.

For this reason, ASIO is expanding its partnerships beyond the traditional – but still critical – law enforcement and security relationships.

In December 2024, for example, ASIO led a body of work by the Five Eyes law enforcement and security agencies examining the radicalisation of minors. The report asked government agencies, the education sector, mental health and social wellbeing services, communities and technology companies for a renewed effort to identify and counter this phenomenon.


FIVE EYES INSIGHTS

Young people and violent extremism: a call for collective action

Five Eyes law enforcement and security agencies are calling for a whole-of-society response to help identify and deal with the radicalisation of minors – especially online – across the Five Eyes nations.

We are increasingly concerned about the radicalisation of minors, and minors who support, plot or undertake terrorist activities. Radicalised minors can pose the same credible terrorist threat as adults, and law enforcement and security agencies cannot address this issue alone.

Minors undertaking violent extremist activities, even if not carrying out an attack, can have lifelong consequences. Governments and providers of health and other support services are already working to address this issue.

We are committed to working with government agencies, the education sector, mental health and social wellbeing services, communities and technology companies as part of a collective effort to identify and counter radicalisation of minors to violent extremism. It is important to work together early as once law enforcement and security agencies need to become involved, it is often too late.

Overview

Violent extremist groups have often been engaged in activities involving the radicalisation of young people (those under 25 years) towards violent extremism. Regardless of their beliefs, young people may become particularly vulnerable to radicalisation and recruitment by violent extremist and terrorist groups.

During the height of the Islamic State of Iraq and the Levant's (ISIL) caliphate, agencies saw many young people and minors (those under 18 years) seeking to join ISIL or undertake violent attacks in support of their home nations. As our threat environments have diversified, security and law enforcement agencies from the Five Eyes nations of Australia, Canada, New Zealand, the United Kingdom and the United States, are collectively seeing minors of varying ideological affiliations in our investigations. In some cases, this has included minors mobilising or planning to mobilise to violence in support of their radicalised ideologies.

Minors can often do what adults can – create and distribute violent extremist content, lead violent extremist groups, recruit and radicalise others to their extremist cause, and even undertake attacks. A minor can have significant influence within extremist contexts, including undertaking or supporting others to conduct violent extremist acts.

While the proportion of young people and minors within our respective counter-terrorism cohorts fluctuates over time, we have seen a significant increase in the role of young people and minors in counter-terrorism cases over the last few years. Many of those who are investigated as minors are also investigated into adulthood due to their violent extremist ideology.

The terms minors and young people are both used in the paper, with the term minors more common. The paper is largely based on information and case studies about minors. Five Eyes partners recognise that the issue of violent extremism, and the drivers of radicalisation, can also apply to young people aged 18–25 years and that is reflected in parts of the paper.

Young people and violent extremism: a call for collective action | 1

Response: countering espionage and foreign interference

ASIO continued to be aggressively postured against espionage and foreign interference, making it more difficult and expensive for foreign spies to operate in Australia.

In one case, ASIO intelligence indicated a foreign intelligence service wanted to harm and possibly kill one or more individuals on Australian soil. Working with our international partners, we determined the plot was part of a broader effort by a regime to eliminate international critics of the foreign government, including activists and journalists.

ASIO's intervention foiled the Australian part of the operation at an early stage.

The Counter Foreign Interference Taskforce investigated many additional cases, including one which resulted in 2 Russia-born Australian citizens being arrested and charged with espionage offences.

Response: Top Secret–Privileged Access

In 2024–25, ASIO advanced the Top Secret–Privileged Access (TS-PA) vetting reforms. The TS-PA Vetting Authority within ASIO serves as a critical safeguard for Australia's most sensitive information and capabilities, protecting against the threat of compromise by trusted insiders and reinforcing the nation's security posture.

By harnessing ASIO's data holdings, capabilities and expertise in security intelligence, the TS-PA Vetting Authority is delivering a robust and consistent approach to vetting, enabling the government to make more informed decisions about an individual's suitability for a security clearance. This, in turn, is facilitating greater mobility and flexibility across the government workforce, while maintaining the highest standards of security assurance.

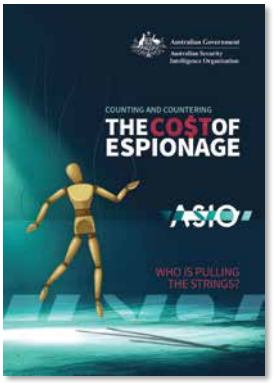
ASIO has consulted with agencies who have highest-level security clearance holders to ensure strong and effective relationships as we continue to advance the TS-PA vetting reforms.

Significant progress was made across the majority of program delivery elements, with ASIO substantially achieving the TS-PA performance target.

Response: influence and impact

Security is a shared responsibility. ASIO's influence and impact agenda helps our stakeholders better understand, identify and manage security threats.

ASIO embraced a more proactive and strategic approach in 2024–25. We partnered with the Australian Institute of Criminology (AIC) to model the impact of espionage. I revealed the AIC's key finding – espionage cost Australia $12.5 billion in one year – when I delivered the 26th Annual Hawke Lecture, launching an ambitious, multi-faceted protective security campaign, *Counting and countering the cost of espionage*.



In this year's Annual Threat Assessment, I declassified elements of ASIO's Security Outlook to 2030. The Outlook is an uncomfortable and frank assessment of emerging and escalating security threats, but I considered it important Australians understood its contents.

The address prompted significant feedback from our stakeholders. Many indicated they would review their security settings in light of the assessment. We tracked a spike in calls to the National Security Hotline relating to matters raised in the speech. And we received a surge of applications from people wanting to work at ASIO.

This response was heartening, given the 3 strategic aims of our influence and impact agenda: to raise awareness of *threats*, to engender *trust* through transparency, and to build our *team* by ensuring ASIO reflects the community it protects.

Conclusion

ASIO's responses and achievements in 2024–25 are reminders that we should not be insecure about our security. The threats facing Australia are substantial but not insurmountable. Foreign intelligence services are sophisticated but not unstoppable. A terrorism threat level of **PROBABLE** does not mean inevitable.



Mike Burgess AM

Director-General of Security



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 systems
- 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.

ASIO cannot just respond to threats, it must anticipate them.

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
- working with partners to enable disruption of 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 2024–25, ASIO pursued its purpose to protect Australia and Australians from threats to their security through 4 security intelligence effects and outcomes in the *ASIO Corporate Plan 2024–28*:

- counter-espionage and foreign interference
- counter-terrorism
- influence and impact
- Top Secret–Privileged Access Vetting.

Part 3 of this report summarises our performance in relation to these priorities during 2024–25.

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 comprehensive oversight and accountability frameworks which underpin and support our commitment to legality and propriety.

ASIO's accountable authority

Mr Mike Burgess AM, the Director-General of Security, was ASIO's accountable authority during the 2024–25 reporting period.

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

		Period as the accountable authority within the reporting period	
Name	**Position title/ position held**	**Date of commencement**	**Date of cessation**
Mr Mike Burgess AM	Director-General of Security	15 September 2019	N/A

Reporting framework

ASIO operates under the Australian Government's outcomes and programs framework.

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

On 29 July 2024, ASIO moved from the Home Affairs portfolio to the Attorney-General's portfolio, and was within the Attorney-General's portfolio for the majority of the 2024–25 reporting period. ASIO returned to the Home Affairs portfolio on 13 May 2025.

It is anticipated this report will be read with broader information provided in the *ASIO Corporate Plan 2024–28* and the *Home Affairs Portfolio Budget Statements 2024–25*, to provide a complete picture of ASIO's planned and actual performance during the financial year.

The alignment between ASIO's purpose, as set out in the *ASIO Corporate Plan 2024–28* and the Outcome and Program in the *ASIO Budget Statement 2024–25*, is shown below.

1 ASIO Budget Statement 2024–25

PORTFOLIO OUTCOME 1

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

PROGRAM 1.1 SECURITY INTELLIGENCE

ASIO operates a single program – Security Intelligence – focused on delivering Outcome 1

2 ASIO Corporate Plan 2024–28

ASIO'S PURPOSE

ASIO protects Australia and Australians from threats to their security

Key performance measures 1–4

3 Annual Performance Statement 2024–25

Report against key performance measures

Organisational structure



Mike Burgess

DIRECTOR-GENERAL OF SECURITY

PRINCIPAL ADVISOR



Mike Noyes

INTELLIGENCE SERVICE DELIVERY



Lisa Alonso Love

ENTERPRISE SERVICE DELIVERY



Gus Gilmore

VETTING SERVICE DELIVERY

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 detailed organisational structure has been deleted from the version of the *ASIO Annual Report 2024–25* tabled in parliament (**Appendix U**).

Our most important asset is our people

Our people are essential to achieving ASIO's mission – to protect Australia and Australians from threats to their security. An increasingly dynamic, diverse and degraded security environment requires a security service full of dynamic, diverse and determined people.

ASIO employees must be able to out-think, out-imagine and outmanoeuvre Australia's adversaries. There is no ASIO type, other than team players who think critically and want to make a difference. They are ordinary Australians who do extraordinary things. ASIO officers have protected the safety and security of Australia and its people for more than 75 years.

ASIO is proud to be formally recognised again for its commitment to diversity and inclusion as a Gold standard employer at the 2025 Australian LGBTQ+ Inclusion Awards. We seek to reflect the diversity of the community we protect. Every ASIO officer brings their unique skills, experience, perspectives and whole selves to work. We are former nurses, trade professionals, scientists, teachers, social workers, librarians, police and journalists. We are proud Aboriginal and Torres Strait Islander peoples, and Australians born here and overseas. We are introverted, extroverted and neurodiverse.

In 2024–25 we recruited new staff to a diverse range of roles in intelligence, technology, vetting and corporate areas. We continue to seek exceptional Australians to join the mission.





3

REPORT ON PERFORMANCE

Annual performance statement 2024–25

Introductory statement

I, as the Director-General of Security and the accountable authority of ASIO, present the 2024–25 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.



Mike Burgess AM

Director-General of Security

Summary of performance against ASIO's purpose

ASIO's 2024–25 annual performance statement details how well we achieved our purpose by protecting Australia and Australians from threats to their security.

During the performance year, ASIO continued to operate in a complex, challenging and changing security environment. Our success relied on our ability to understand the environment, identify and understand the threats it presents, and convert this understanding into actionable insights and impactful advice.

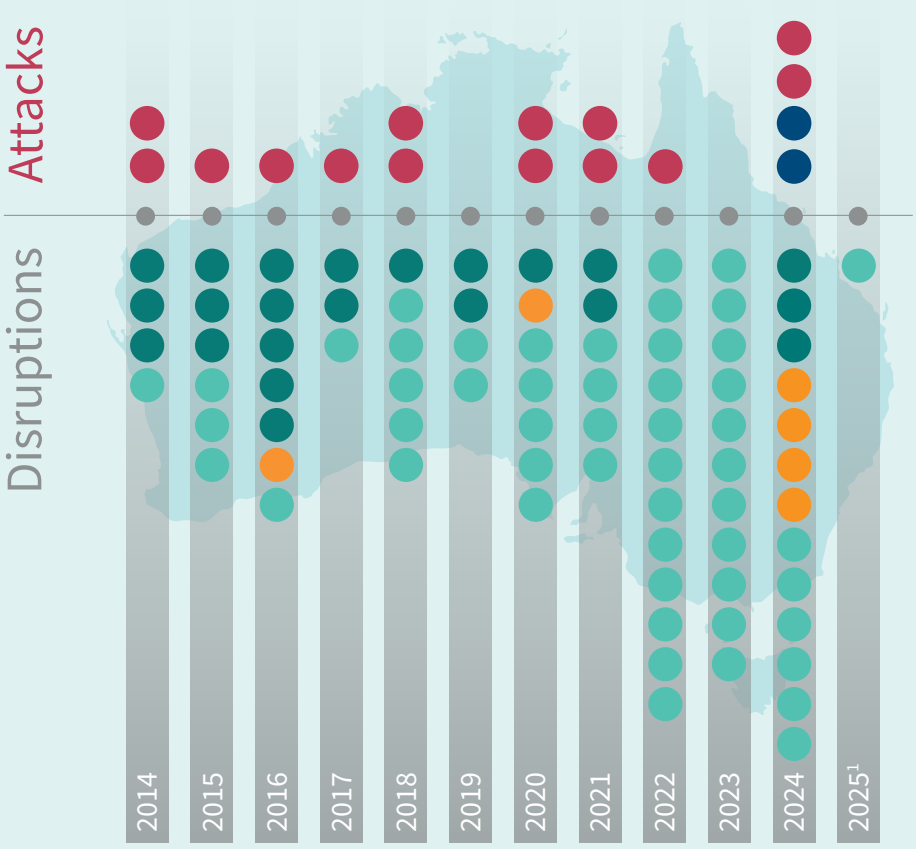
Our ability to respond to the security environment is evidenced in achieving 3 of 4 performance measures in the *ASIO Corporate Plan 2024–28*, with one performance measure substantially achieved.

ASIO achieved and delivered significant outcomes against all counter-espionage and foreign interference, counter-terrorism, and influence and impact performance measures.

Significant progress was made to implement the Top Secret–Privileged Access (TS-PA) Vetting capability, including across the majority of program delivery elements. ASIO substantially achieved the TS-PA performance target.

For national security reasons, aspects of ASIO's 2024–25 annual performance statement have been removed from this annual report, as allowed by the application of section 105D of the PGPA Act. Additional details of ASIO's 2024–25 annual performance statement are included in the classified appendices to the *ASIO Annual Report 2024–25* (**Appendix T**).

Disruptions and attacks



Domestic terrorist attack

Terrorism directed by a foreign state-actor

Major counter-terrorism disruption (Religiously Motivated Violent Extremism)

Major counter-terrorism disruption (Ideologically Motivated Violent Extremism)

Major espionage and foreign interference disruption

[1] Indicates disruptions and attacks reported up to 30 June 2025.

Measuring performance

ASIO's performance is measured through a combination of quantitative and qualitative methods, including defined targets, case studies, stakeholder feedback and identified milestones.

In accordance with the *ASIO Corporate Plan 2024–28*, assessment of the impact of our operational activities and advice relating to counter-espionage and foreign interference, and counter-terrorism (measures 1–2) is based on quantitative data and qualitative feedback from ASIO's stakeholder survey, case studies, and the results of ASIO's biannual internal performance tracking.

The stakeholder survey draws on quantitative and qualitative data to support the reliability and verification of ASIO's performance results.

In 2024–25, ASIO removed policy measures for counter-espionage and foreign interference and counter-terrorism to place a greater emphasis on ASIO's operational outcomes. The performance statement provides comparison against the operational outcomes and an average of the policy and operational outcomes from previous years, noting neither of these are exactly the same, and therefore cannot provide a strict 'like-for-like' comparison.

The annual survey for 2024–25 was sent to 56 key stakeholders, with 37 responses received from a range of Commonwealth entities and state law enforcement partners who are:

- ongoing, frequent recipients of ASIO counter-espionage and foreign interference and/or counter-terrorism advice
- engaged in operational activities, managing security risks, disruption activities, and/or developing policy responses related to counter-espionage and foreign interference and/or counter-terrorism.

The 2024–25 questionnaire asked stakeholders to numerically rate the level of impact ASIO advice had on their decision-making relating to counter-espionage and foreign interference, and counter-terrorism as applicable to their role. In addition to the rating, the questionnaire sought qualitative feedback on the impact of ASIO operational activities and advice across counter-espionage and foreign interference and/or counter-terrorism. Examples of how ASIO advice was useful in each of these activities and any improvements ASIO could make to have a higher impact were also sought.

To further support analysis of the performance results, a cross-section of these 56 key stakeholders were invited to interview.

Stakeholders were asked the same questions during interviews, with the opportunity for the interviewer to ask follow-up questions. Stakeholders were also asked about any requirements or expectations of ASIO over the next year, and what ASIO could do to increase its value to their organisation.

ASIO's performance and impact across counter-espionage and foreign interference, and counter-terrorism was rated on a 9-point scale. Ratings 1 to 3 indicated **LOW** impact, 4 to 6 indicated **MEDIUM** impact and 7 to 9 indicated **HIGH** impact.

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

The number of ratings in each category were aggregated, and divided by the total number of responses to derive the percentage of stakeholders who rated ASIO's performance as **LOW**, **MEDIUM** and **HIGH** impact.

In addition, case studies were used to demonstrate the depth and breadth of ASIO operational activities in understanding, disrupting and hardening the environment from espionage and foreign interference and terrorism, reducing harm to Australia and Australians.

Results from ASIO's biannual internal performance tracking were considered to validate and support the interpretation of the quantitative survey results.

Assessment of our performance against our influence and impact measure (measure 3) has been informed by case studies identified early in the performance year, and provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's activities and advice for our stakeholders, resulting in outcomes that contribute to protecting Australia and Australians from threats to their security.

ASIO's use of case studies are not a standalone measure and are linked to other sources of performance data, including examples raised by stakeholders as part of the stakeholder survey.

Assessment of our performance against our Top Secret–Privileged Access Vetting delivery measure (measure 4) has been informed by a range of inputs including program governance and oversight arrangements, assessment of benefits realisation, stakeholder feedback, the development of key enabling partnerships, the onboarding of capabilities, and program delivery metrics such as budget and timeframe.

Counter-espionage and foreign interference

Impact of ASIO's counter-espionage and foreign interference operational activities and advice

Measure	The percentage of key stakeholders who confirm our counter-espionage and foreign interference advice had a MEDIUM or HIGH 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. Case studies which demonstrate the delivery of an operational counter-espionage and foreign interference outcome.
Overall result	ACHIEVED
Source	*ASIO Corporate Plan 2024–28* (p.16) | *PBS 2024–25,* Outcome 1 (table 2.1.2)

How performance was assessed	Result
a. Annual survey of ASIO's key stakeholders.	ACHIEVED
b. ASIO's assessment of the significant outcomes – understand, harden and disrupt – from our counter-espionage and foreign interference activities and the impact of protecting Australia and Australians from threats to their security.	ACHIEVED

Results and analysis

ASIO has countered espionage and foreign interference by protecting Australia from threats posed by foreign intelligence services and their proxies seeking to undermine and exploit Australia's democratic systems, institutions and values. ASIO has collected intelligence on, and investigated, threats targeting Australian Government, defence, political and other national interests. In 2024–25, ASIO continued to focus considerable resources to understand the threat and harden the environment.

Annual survey of ASIO's key stakeholders

100 per cent of survey respondents reported that ASIO's advice on counter-espionage and foreign interference had a **MEDIUM** or **HIGH** impact on their decision-making, exceeding the 90 per cent **MEDIUM-HIGH** target.

90 per cent of respondents considered ASIO's advice had a **HIGH** impact on their decision-making, informing operational activities, managing security risks and disrupting activities that threatened Australia's security.

These stakeholders considered that ASIO's advice was timely and relevant, practical, focused and provided or enabled exercisable options, and directly informed and shaped decision-making.

When compared against the previous operational measure and an average of the previous operational and policy performance measures, the percentage of stakeholders rating ASIO's counter-espionage activities and advice as **MEDIUM-HIGH** has increased year-on-year to a high-point of 100 per cent for both 2023–24 and 2024–25.

The percentage of stakeholders rating ASIO's advice as **HIGH** (90 per cent) has declined in 2024–25, from the 2023–24 peak of 100 per cent **HIGH** (compared against the operational measure) or 94 per cent **HIGH** (compared against an average of the policy and operational measures).

In 2024–25, stakeholders provided feedback that ASIO's intelligence and advice was critical to a number of key operations and disruptions, and that ASIO's counter-espionage advice had informed their policies, security posture, and approach to managing risk.

2020–21 result	2021–22 result	2022–23 result	2023–24 result	2024–25 result
Operational impact				
89% MEDIUM or higher	80% HIGH 92% MEDIUM or higher	68% HIGH 96% MEDIUM or higher	100% HIGH	
Target				
70% MEDIUM	80% MEDIUM	80% HIGH	90% MEDIUM-HIGH	100% MEDIUM or higher 90% HIGH Target: 90% MEDIUM-HIGH
Policy impact				
100% MEDIUM or higher	73% HIGH 97% MEDIUM or higher	64% HIGH 95% MEDIUM or higher	88% HIGH 100% MEDIUM or higher	
Target				
70% MEDIUM	80% MEDIUM	80% HIGH	90% MEDIUM-HIGH	

Assessment of the impact of ASIO's operational activities and advice

ASIO's advice in 2024–25 provided context, was relevant and practical, and influenced decision-making.

Examples demonstrating the impact of ASIO's counter-espionage and foreign interference operational activities and advice include the following.

- ASIO operational activity to understand the security relevance of an individual engaged in foreign interference, including attempted cultivation of government employees, ensured this behaviour on behalf of a foreign adversary was mitigated.
- Investigations led to the disruption of the use of consultancy firms by foreign adversaries to target individuals with access to privileged, sensitive or classified information.
- ASIO published products on security threats to the federal election, including from foreign interference, espionage and sabotage, which built greater awareness of the threat of foreign interference across electoral and government stakeholders. This advice enabled electoral authorities to develop mitigation strategies, and informed and supported their decision-making.
- ASIO increasingly provided advice in relation to security risks presented by emerging technology. In this context, ASIO published product which instigated a state government to take immediate action to mitigate a threat.
- ASIO raised government stakeholder awareness of the insider threat to generate reporting and build up and to help equip government departments to manage their insider threats. ASIO provided briefs to government departments and agencies on personnel security and insider threat advice and mitigation. ASIO continues to engage with state and territory governments to promulgate protective security messaging.
- In support of economic security, ASIO continued to provide advice to the Department of the Treasury on a range of relevant Foreign Investment Review Board cases, including advice on threats to security concerning critical assets and technology, and sensitive Defence sites.



Furnishing a prejudicial Security Clearance Suitability Assessment

In October 2024, ASIO furnished a prejudicial Security Clearance Suitability Assessment (SCSA) in relation to an individual assessed to have conducted sabotage of an Australian Government capability. The SCSA provided the assessment that was acted on by an Australian Government agency in revoking the individual's clearance and terminating their employment.

Countering espionage

ASIO provided advice to government regarding an Australian person conducting activities on behalf of a foreign intelligence service overseas. The individual has an extensive network, including Australian and foreign government officials in the country they reside in, and was using these connections to obtain information and contacts to provide to the foreign intelligence service. Our advice resulted in an uptick in contact reporting and defensive briefings to Australian Government personnel who had been in contact with this individual.

Counter-terrorism

Impact of ASIO's counter-terrorism operational activities and advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a MEDIUM or HIGH impact on their decision-making in relation to informing counter-terrorism operational activities, managing security risks and disrupting activities that threatened Australia's security. Case studies which demonstrate the delivery of an operational counter-terrorism outcome.
Overall result	ACHIEVED
Source	*ASIO Corporate Plan 2024–28* (p.17) | *PBS 2024–25,* Outcome 1 (table 2.1.2)

How performance was assessed	Result
a. Annual survey of ASIO's key stakeholders.	ACHIEVED
b. ASIO's assessment of the significant outcomes – understand, harden and disrupt – from our counter-terrorism activities and the impact of protecting Australia and Australians from threats to their security.	ACHIEVED

Results and analysis

ASIO has countered terrorism by protecting Australians from religiously motivated and ideologically motivated violent extremism by anticipating threats and responding to changes in the security environment. ASIO's intelligence collection, investigation and assessment efforts enabled ASIO to identify and understand the threats we face, and enabled the provision of impactful advice that hardened the environment against violent extremism.

Annual survey of ASIO's key stakeholders

100 per cent of survey respondents reported that ASIO's counter-terrorism advice had a **MEDIUM** or **HIGH** impact on their decision-making, exceeding the 90 per cent **MEDIUM-HIGH** target. Of this, 85 per cent of respondents considered ASIO's advice had a **HIGH** impact on their decision-making informing operational activities, managing security risks and disrupting activities that threatened Australia's security as it related to counter-terrorism.

The percentage of **HIGH** impact ratings in 2024–25 is higher than in any of the previous 4 years, with commentary from some survey respondents noting a positive improvement in their interaction and relationship with ASIO. The percentage of stakeholders rating advice as **MEDIUM** or **HIGH** in 2024–25 (100 per cent) is consistent with previous years.

In 2024–25, stakeholders noted that ASIO made key contributions to their operations, arrests, prosecutions and diversion activities over the period. Stakeholders considered ASIO to be an excellent counter-terrorism partner, making critical contributions to ensure community safety. Stakeholders also provided feedback that ASIO's advice was used to inform strategies and priorities, make informed decisions on risk, and to uplift situational awareness.

2020–21 result	2021–22 result	2022–23 result	2023–24 result	2024–25 result
Operational impact				
58% HIGH 93% MEDIUM or higher	84% HIGH 100% MEDIUM or higher	78% HIGH 96% MEDIUM or higher	71% HIGH 100% MEDIUM or higher	
Target				
80% MEDIUM	80% MEDIUM	80% HIGH	90% MEDIUM-HIGH	100% MEDIUM or higher 85% HIGH Target: 90% MEDIUM-HIGH
Policy impact				
56% HIGH 100% MEDIUM or higher	71% HIGH 100% MEDIUM or higher	63% HIGH 100% MEDIUM or higher	71% HIGH 94% MEDIUM or higher	
Target				
80% HIGH	80% HIGH	80% HIGH	90% MEDIUM-HIGH	

Assessment of the impact of ASIO's operational activities and advice

ASIO's advice in 2024–25 provided context, was relevant and practical, and influenced decision-making.

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

- ASIO threat advice informed whole-of-government security planning for major events and official travel, including Australia's participation in ANZAC Day events in Türkiye and France, the Paris 2024 Olympic and Paralympic Games, T20 World Cup, the 2024 United Nations Climate Change Conference, Commonwealth Heads of Government Meeting, and Asia-Pacific Economic Cooperation.
- ASIO advised Australian Government partners about imminent, persistent and emerging terrorist threats, supported the activities of National Intelligence Community (NIC) counter-terrorism partners, and informed the Department of Foreign Affairs and Trade's advice and assessments to protect Australians and Australia's diplomatic missions from terrorist threats overseas.
- ASIO involvement in counter-terrorism training bolstered ASIO and law enforcement readiness for a major terrorism incident response. ASIO supported and/or participated in 22 Commonwealth, state or territory counter-terrorism related training courses conducted around Australia, training over 300 police officers, Australian Defence Force personnel, and others in various aspects of counter-terrorism and response. ASIO also supported a variety of exercises and preventative security operations supporting major events such as the visit of His Majesty King Charles III to Australia, and the Land Forces Exposition in Victoria in September 2024.
- ASIO has produced a range of products on the radicalisation of young people. ASIO is a member of the Australia – New Zealand Counter-Terrorism Committee Youth and Mental Health Advisory Group (the Group) and regularly briefs the Group on areas of mutual interest. In November 2024, ASIO presented to the Group, providing an overview of ASIO's minors in counter-terrorism research project for partner awareness. This specific engagement provided uplift to partner agencies through increased awareness of radicalisation indicators and pathways for minors.

- In October 2024, ASIO engaged with a state government department and presented on the security environment in Australia to support its ability to identify potential counter-terrorism indicators in students. Following this engagement, the department sought ASIO advice on the impact of the Middle East conflict on communities of repatriated families. The ongoing engagement sought by the department demonstrates the value placed on ASIO's advice.
- ASIO worked closely with partners following the raising of the national terrorism threat level to **PROBABLE** in August 2024, particularly with law enforcement to inform its protective security mitigations and postures. This included working with the Australian Federal Police (AFP) and the Australian Electoral Commission in the lead up to, and during, the 2025 Federal Election, providing threat and security assessment and advice to AFP intelligence teams to inform threat mitigation and operational planning.

ASIO working with law enforcement partners

ASIO worked closely with Joint Counter Terrorism Teams in states and territories to respond to specific threats, including providing intelligence support to counter-terrorism investigations and 4 major counter-terrorism disruptions. In one instance, ASIO engagement with a foreign partner proved critical in identifying an individual planning to conduct an act of politically motivated violence in Australia. Subsequent engagement with the Joint Counter Terrorism Team led to the disruption of the individual.

Cancellation of visa due to security risks

In October 2024, the Director-General recommended that the Department of Home Affairs cancel a foreign national's visa due to an adverse security assessment by ASIO. After analysis of intelligence and investigative activity spanning several months, ASIO concluded the person was likely a risk to security if allowed to stay in Australia. The individual was subsequently placed in immigration detention.

In 2024–25
172,788
total

Access security assessments finalised



162,588

Access to places

ASIC, CIBC, Flight Crew, MSIC, NSSIC[2]



10,200

Access to substances

AN, ANSTO, NHSC, radiological material and equipment (QOPT)[3]



0

Access to events

For 2024–25, no new accreditation schemes were introduced and there were no major events requiring event access assessments.

57,187
finalised

Personnel security assessment referrals finalised



51,658

Baseline, Negative Vetting (NV) 1 and 2 clearances

Increased from 44,315 assessments finalised in 2023–24



5,529

Positive Vetting (PV) clearances

Increased from 3,340 assessments finalised in 2023–24

[2] Aviation Security Identification Card (ASIC), Critical Infrastructure Background Check (CIBC), Flight Crew Licence (Flight Crew), Maritime Security Identification Card (MSIC), and Naval Shipbuilding and Sustainment Identity Card (NSSIC)

[3] Ammonium Nitrate (AN), Australian Nuclear Science and Technology Organisation (ANSTO), and National Health Security Check (NHSC)

Influence and impact

ASIO's delivery of impactful and influential Organisational activities and advice

Measure	Case studies which demonstrate the influence and impact of ASIO activities and advice, resulting in outcomes that contribute to protecting Australia and Australians from threats to their security.
Overall result	ACHIEVED
Source	*ASIO Corporate Plan 2024–28* (p.18)

How performance was assessed	Result
The influence and impact measure relies on demonstration, via at least one case study, of ASIO's delivery of impactful and influential activities and advice resulting in outcomes that contribute to protecting Australia and Australians from threats to their security. Case studies have been chosen on the basis of their demonstration of the impact of ASIO activities and advice with consideration to protecting sensitive tradecraft, capabilities and information. ASIO has been proactive in its advice to government and industry, leveraging our capabilities and insights to help stakeholders better understand, identify and manage security threats.	ACHIEVED

Results and analysis

The scale and sophistication of the threats facing Australia require ASIO to be proactive in its advice to government, business, academia, industry and the public. ASIO leveraged its capabilities and insights to help stakeholders better understand, identify and manage security threats. ASIO promoted security awareness and strengthened security maturity by providing expert insights and impactful advice.

The following case studies have been selected as they demonstrate a range of scenarios where ASIO has delivered impactful and influential activities and/or advice.

Annual Threat Assessment

The Director-General's Annual Threat Assessment raises awareness of security threats. The increase in leads following the threat assessment is one indicator showing demonstrable impact. In 2025 there was a 12 per cent increase in national security leads the week after the assessment (compared to the weekly average for 2024). This included a number of high-quality leads. ASIO continues to operate in a heightened lead environment relative to previous years.

Raising the national terrorism threat level to PROBABLE

ASIO raised the national terrorism threat level to **PROBABLE** in August 2024. We provided advice to a spectrum of government and private sector stakeholders to inform their policy and operational considerations. This advice was also provided to the public. ASIO's assessments and briefings fed into the Department of Home Affairs' development of an updated countering violent extremism and terrorism strategy.

Countering insider threats

We continue to engage with Australian Government departments and agencies to identify potential insider threats to national security. ASIO worked with partners to educate and support Commonwealth departments' insider threat programs including educating clearance holders on identifying national security threats, referring potential threats to ASIO, and working together to mitigate, manage and enable disruption of national security threats involving Australian Government clearance holders.

Security Outlook 2030: the age of surprise and time for deterrence

ASIO prepared a strategic assessment on the possible future outlook for our security environment to inform ASIO leadership, staff and Australian Government partners. We undertook active engagement to communicate the key assessment lines of the report to achieve maximum impact and we received positive feedback on the utility of the report from diverse stakeholders.

ASIO published a lower-classified version of the assessment to reach and inform a wider audience than the initial more highly-classified version. Declassified elements were included in the Director-General's Annual Threat Assessment in February 2025. Multiple stakeholders noted the utility of the unclassified futures assessments in the Director-General's Annual Threat Assessment as well as the lower-classified version of the strategic assessment, providing positive feedback and seeking opportunities to engage further with ASIO. ASIO's assessments on the future outlook of the security environment informed a number of policy settings across government.

Middle East conflict and its implications for Australia

ASIO has been closely monitoring events in the Middle East since the 7 October 2023 terrorist attack by Hamas. Hamas's attack, and Israel's response, continued to resonate across the spectrum of interest groups and communities in Australia. ASIO has provided ongoing advice to government and law enforcement on a range of security issues stemming from the conflict. This included advice to strategic, policy and operational partners, designed to inform their own responses to the evolving security environment. ASIO's official assessments and the public remarks by the Director-General have been quoted and used extensively in media, policy discussions, and academic literature.

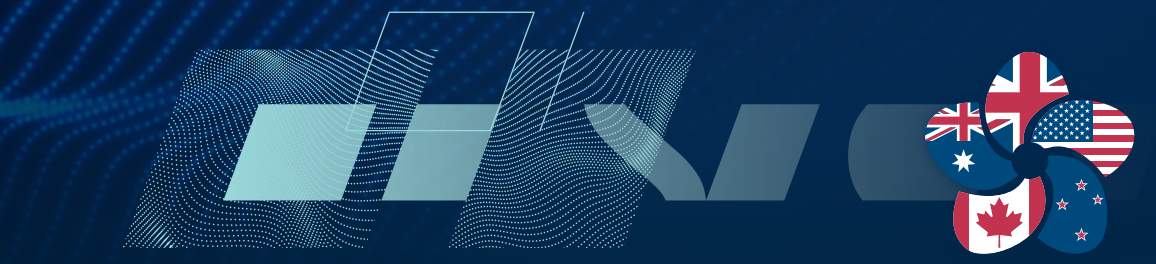
Defending AUKUS

In 2024–25, ASIO focused on the protection of AUKUS capabilities by working closely with domestic and foreign partners to prevent clandestine intelligence operations targeting the nuclear-powered submarine enterprise.

Community interference

ASIO responded to attempts by foreign governments to repatriate and intimidate members of diaspora communities in Australia. Our response has been designed to harden both individuals and community groups from this threat. Much of our activity is conducted in close collaboration with federal and state law enforcement. In addition to hardening the security environment in Australia, this activity is supporting investigations which will ultimately enable disruption of foreign governments and their onshore proxies' targeting of Australian interests.

In 2024–25 we embraced a more proactive and strategic approach to our influence and impact agenda. We will continue to progress ambitious, multi-faceted campaigns in 2025–26, including through the ***Counting and countering the cost of espionage*** campaign, to help our stakeholders better understand, identify and manage security threats. This will advance the 3 strategic aims of our influence and impact agenda: to raise awareness of ***threats***, to engender ***trust*** through transparency, and to build our ***team*** by ensuring ASIO reflects the community it protects.



ASIO leads Five Eyes focus on the radicalisation of minors

In December 2024, ASIO and the Australian Federal Police led and published *'Young people and violent extremism: a call for collective action'*. This insight paper was the first of its kind, being a collaborative initiative of Five Eyes security and law enforcement agencies. It calls for a whole-of-society response to help identify and deal with the radicalisation of minors across our collective nations.

ASIO, the Australian Federal Police and our other partners in counter-terrorism are increasingly concerned about the radicalisation of minors, and minors who support, plan or undertake terrorist activities. Radicalised minors can pose the same credible terrorist threat as adults. Minors undertaking violent extremist activities, even if not carrying out an attack, can have lifelong consequences for the child and those around them. The online environment provides extensive opportunities for minors to access extremist material. Violent extremist content is more accessible, more digestible and more impactful than ever before.

This availability makes radicalisation to violent extremism a process which can take place entirely online, at times without any offline indications, leaving minors who are regularly online vulnerable.

Governments and service providers are already working to address this issue. We are committed to working with government and law enforcement agencies, the education sector, mental health and social wellbeing services, communities, and technology companies as part of a collective effort to identify and counter radicalisation of minors to violent extremism. It is important to work together early, as once law enforcement and security agencies need to become involved it is often too late.

Top Secret–Privileged Access Vetting

Measure	High assurance and transferable security clearances are issued to Australia's highest-cleared workforce.
Overall result	SUBSTANTIALLY ACHIEVED
Source	*ASIO Corporate Plan 2024–28* (p.19) | *PBS 2024–25,* Outcome 1 (table 2.1.2)

How performance was assessed	Result
Qualitative and quantitative analysis of the capability is informed via a range of inputs, including program governance and oversight arrangements, assessment of benefits realisation, stakeholder feedback, the development of key enabling partnerships, the onboarding of capabilities, and other program delivery metrics such as budget and timeframe.	SUBSTANTIALLY ACHIEVED

Results and analysis

The program's performance methodology encompassed inputs from program governance and oversight arrangements, assessment of benefits realisation, stakeholder feedback, the development of key enabling partnerships, the onboarding of capabilities, and delivery metrics such as budget and timeframe.

The Top Secret–Privileged Access (TS-PA) reforms strengthen Australia's national security by enhancing access controls, improving insider threat detection, and increasing information sharing to protect against the risk of compromise by trusted insiders.

The TS-PA reforms centralise and standardise the highest-level vetting functions within the TS-PA Vetting Authority. Early benefits have delivered greater efficiency, information sharing, cohesion and consistency. By leveraging ASIO's security intelligence functions, holdings and capabilities, a holistic assessment of an individual's suitability to hold a TS-PA security clearance has been achieved.

In a phased approach ASIO has refined its productivity metrics and objectives, established supporting policy frameworks, and enhanced enabling capabilities.

As the majority of inputs were assessed as achieved for 2024–25, ASIO substantially achieved the performance measure for delivering the TS-PA Vetting program.

As the TS-PA reforms transition from a capability development focus to a mature operational model, ongoing capability targets and qualitative key performance indicators will be progressively implemented from 2025–26 through 2027–28 to measure performance.

Some information on TS-PA performance has been outlined in **Appendix T**[4] at the SECRET level to balance the need for transparency against the risk of introducing vulnerabilities in the TS-PA vetting capability which could be exploited by foreign adversaries.

Program governance and oversight arrangements

ASIO continues to work closely with the Office of National Intelligence (ONI) to implement the National TS-PA Capability (the Capability). The Capability is subject to robust oversight and governance, with internal and external layers of review and accountability in place to ensure its effective operation.

The Capability is subject to oversight from the Office of the Inspector-General of Intelligence and Security (OIGIS), which conducts annual inspections of the TS-PA Vetting Authority. In 2024–25, the OIGIS completed its second inspection, which focused on the progress of the TS-PA reforms over the last 12 months.

Benefits realisation

The Capability continues to mature and in 2025–26 onwards focus will shift to achieving the planned benefits and delivering expected outcomes.

ASIO worked with the Australian Government Security Vetting Agency (AGSVA), within the Department of Defence, to progress planning to transition agencies from AGSVA Positive Vetting (PV) arrangements to the TS-PA Vetting Authority. This will expand benefits realisation to a greater number of stakeholder agencies, and ensures alignment with the Defence Strategic Review recommendation for the transfer of Defence authorities to the TS-PA Vetting Authority.

Overall, the TS-PA Capability is on track to deliver its planned benefits to government, with a focus on transferability, consistency, quality and assurance.

[4] Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, components of the annual performance statement have been deleted from the version of the *ASIO Annual Report 2024–25* tabled in parliament.

Stakeholder feedback

Throughout the reporting period, the TS-PA Vetting Authority engaged closely with stakeholders, including Chief Security Officers, AGSVA and other Commonwealth agencies.

ASIO is supporting AGSVA in responding to TS-PA implementation-related inquiries from PV security clearance holders and members of the public.

The Capability has hosted and participated in various whole-of-government forums which have provided opportunities for stakeholders to raise concerns or questions about the transition from PV to TS-PA security clearances.

The Capability is collaborating with PV and TS-PA security clearance sponsoring agencies to support their transition to the TS-PA Vetting Authority. This includes through the development of tailored transition plans that cater to each agency's unique requirements, and in-depth briefings on key topics.

ASIO has also published new content on its website regarding the TS-PA reforms, including a dedicated TS-PA Vetting Authority page.

Development of key enabling partnerships

The key enabling partnerships necessary to deliver on this measure have progressed as scheduled, following enterprise-endorsed approaches to partnerships and authority to engage with affected stakeholders provided by the Capability's governing forums.

Onboarding of capabilities

ASIO is implementing a phased onboarding strategy for new capabilities, prioritising maturity and sustainability to meet TS-PA security clearance requirements while maintaining the integrity of its broader security functions.

A comprehensive Transition Plan is being developed to support sponsor agency transitions. A number of projects have been established to build capability and capacity, including initiatives aimed at strengthening policy, legal and partnerships; enhancing workforce and culture; advancing technology, data and analytics; and upgrading facilities, infrastructure and systems.

Overall, the Capability is on track to deliver a quality-assured, standardised, and scalable TS-PA vetting capability for the Commonwealth.

Program delivery metrics – timeframe

ASIO is committed to transferring all Commonwealth PV authorities to the TS-PA Vetting Authority by the agreed government timelines. As such, ASIO is actively managing multiple parallel workforce, system and infrastructure projects to deliver the timely provision of necessary business capabilities.

While ASIO is proactively managing dependencies between these projects, external factors such as the state of the labour market, the availability of skills and resources, and the timelines for delivery of external programs may impact the transition timeline.

Report on financial performance

The 2024–25 financial statements report a $104.52 million operating deficit compared with a $111.46 million operating deficit the previous financial year. ASIO's 2024–25 operating funding from government was $598.59 million compared to $534.08 million in 2023–24. The 2024–25 result includes items such as depreciation and amortisation expenses (including for the right-of-use leased assets), which are non-cash in nature. ASIO does not receive operating funding for non-cash items.

After adjusting for these items, the 2024–25 operating result is a deficit of $11.04 million (approved $9.21 million). The additional $1.84 million relates to technical accounting losses from the disposal of assets, write-offs and impairment.

In 2024–25 ASIO received $150.61 million in capital funding through the departmental capital budget for asset replacement and equity injections. This compares to $135.27 million in 2023–24. This funding has been applied to the necessary development, enhancement and replacement of assets to support ASIO's operational effectiveness in the increasingly complex security and technology environments.

A table summarising ASIO's total resources for 2024–25 is provided at **Appendix A**.

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



4

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); 3 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).

In 2024–25, ASIO refined its enterprise management and governance practices, including:

- reviewing our governance arrangements and refreshing our processes to ensure they remain fit for purpose
- continuing to mature our approach to enterprise risk management in line with the Commonwealth Risk Management Maturity Model
- strengthening ASIO's preparedness to respond in the event of crisis through strategic planning and activities.

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 related 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 related to or impacting on ASIO's influence agenda, and gives account of performance against ASIO's objectives and endorsed lines of effort.



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 functions include reviewing ASIO's administration and expenditure, national security legislation, and any matter referred to it by the responsible Minister in relation to ASIO (and other intelligence agencies).

In 2024–25, ASIO provided a written submission to the PJCIS Review of Administration and Expenditure No. 23 (2023–24).

Senate Legal and Constitutional Affairs Committee

In 2024–25, ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate Estimates process on 4 November 2024, 25 February 2025 and 27 March 2025.

ASIO's evidence to the committee can be found in the estimates Hansard for those days (refer to www.aph.gov.au).

ASIO also contributed to the following Senate Legal and Constitutional Affairs Committee inquiries.

- ASIO provided a written submission to the Senate Legal and Constitutional Affairs Legislation Committee as part of its inquiry into the Criminal Code Amendment (Hate Crimes) Bill 2024.
- ASIO appeared before the Senate Legal and Constitutional Affairs References Committee as part of its inquiry into right-wing extremist movements in Australia.

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 and inquiries of ASIO's investigative and operational functions, as well as investigating complaints received about ASIO.

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 retains statutory powers akin to those of a standing royal commission.

During 2024–25 the IGIS regularly inspected activities across our operational and analytical functions, and investigated complaints received by the IGIS. We are committed to acting with legality and propriety, and in 2024–25 we continued to respond to recommendations where the IGIS identified concerns or areas requiring improvement.

We continued to support the IGIS's important work throughout 2024–25 by proactively briefing IGIS staff on a number of operational matters, including new capabilities and initiatives.

National Anti-Corruption Commission

The National Anti-Corruption Commission (NACC) is an independent Commonwealth agency that commenced operations on 1 July 2023. It has broad jurisdiction to detect, investigate and report on serious or systemic corruption across the Commonwealth public sector. The NACC forms an important part of ASIO's multifaceted integrity framework.

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 powers to access all relevant material, including classified information, and can determine its own review process which usually includes an issues paper, consultation meetings, seeking submissions from interested parties, and public and/or private hearings. INSLM reports are tabled in parliament.

During 2024–25, ASIO made a submission to the INSLM's review of the espionage, foreign interference, sabotage and theft of trade secrets offences (Division 82 and Part 5.2 *Criminal Code Act 1995*).

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 the Department of 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 2024–25 reporting period.

Independent Reviewer of Security Clearance Decisions

The Independent Reviewer of Security Clearance Decisions reviews certain security clearance decisions for persons who did not hold an existing security clearance nor were Commonwealth employees immediately before the original security clearance decision was made. Independently reviewable decisions are decisions made following internal review, to deny a security clearance, revoke a security clearance, or impose or vary a condition on a security clearance.

Appendix D provides the Independent Reviewer of Security Clearance Decision's annual report for the 2024–25 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.

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.

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 are operating as intended. These efforts also serve to ensure ASIO is positioned to meet current and future security challenges.

Internal audit function

ASIO's internal audit function provides assurance on the effectiveness of governance arrangements, risk management frameworks and internal control mechanisms. Through the application of a systematic and disciplined evaluation methodology, this function supports the establishment and maintenance of robust internal control and governance frameworks, facilitating effective and efficient operations.

In accordance with organisational security policies and operational considerations, the internal audit function is afforded unrestricted access to all ASIO premises, work areas, documentation and information necessary to discharge its responsibilities.

During the reporting period, ASIO conducted a comprehensive program of compliance audits and performance reviews, aimed at assessing adherence to established policies, procedures and standards, and identifying opportunities for improvement.

Compliance function

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

The centralised compliance function ensures a formal, structured approach to supporting compliance in ASIO. It performs an important role in demonstrating ASIO's transparency and commitment to further embedding a culture of compliance within ASIO.

ASIO Audit and Risk Committee

The ASIO Audit and Risk Committee is an independent advisory body, established to provide 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 in accordance with a formally established charter, which outlines its functions and responsibilities as mandated by section 45 of the PGPA Act and section 17 of the Public Governance Performance and Accountability Rule 2014.[5]

In accordance with its charter, the committee comprises up to 5 external members, including an independent chairperson, as well as observers from the Australian National Audit Office (ANAO).[6] The committee's membership is characterised by a diverse range of relevant qualifications, expertise and experience pertinent to ASIO's operations. This membership includes a minimum of one member with accounting or related financial management expertise, as well as a demonstrated understanding of public sector accounting and auditing standards. Upon appointment, committee members participate in a comprehensive induction briefing on ASIO's governance framework and operational context.

During this reporting period, the committee met on 5 occasions, comprising regular quarterly meetings and an extraordinary meeting dedicated to the review of the financial statements. Each meeting achieved a quorum, ensuring the committee's deliberations were valid and effective.

A copy of the charter and information about the members, including qualifications and remuneration, is available at **Appendix R**.

[5] 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 *ASIO Annual Report 2024–25* tabled in parliament (**Appendix R**).

[6] 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 *ASIO Annual Report 2024–25* tabled in parliament (**Appendix R**).

Fraud control and management

ASIO has zero tolerance for fraudulent behaviour. We treat both suspected and actual fraud seriously and take all reasonable measures to prevent, detect and investigate fraudulent behaviour. ASIO's *Fraud and Corruption Control Plan* documents our approach to fraud and corruption awareness, prevention, detection, reporting and investigation, and our commitment to ensuring efficient, effective and ethical use of resources. This approach includes the information and data we collect as well as the resources received from government. Our fraud and corruption prevention measures are in line with the *Commonwealth Fraud and Corruption Control Framework 2024*.

During the reporting period ASIO conducted fraud pressure testing on a sample of controls identified in our *Fraud and Corruption Risk Register*. This testing allowed us to identify fraud vulnerabilities and determine the effectiveness of our controls.

As part of this framework, all staff must complete mandatory eLearning on ethics and accountability, including modules on fraud and corruption, during induction and then at least every 3 years thereafter.

ASIO's *Fraud Strategy Statement 2024* (www.asio.gov.au/resources/strategy-and-policy/asio-fraud-strategy-statement) provides further information on our fraud and corruption control and management arrangements.

Significant legal matters affecting ASIO's business

During 2024–25, ASIO continued to be involved in numerous legal proceedings in courts and tribunals, and in inquisitorial settings. Matters have included prosecutions, civil law disputes, applications for judicial and merits review, a judicial inquiry and applications for post-sentence orders.

There were no judicial or tribunal decisions during the period that have had a significant effect on ASIO operations.

Merits reviews

ASIO was involved in proceedings before the former Administrative Appeals Tribunal and the newly established Administrative Review Tribunal. These proceedings included reviews of ASIO security assessments relating to eligibility for visas, security clearances and passports. Over the reporting period ASIO was also involved in Tribunal reviews of National Archives access decisions in which exemptions had been made to protect ASIO material from release.

Criminal prosecutions, other civil law matters and proceedings, inquiries and post-sentence order applications

ASIO was involved in a range of other legal matters and proceedings during the reporting period. These included:

- in collaboration with our law enforcement partners and prosecuting authorities – and with appropriate protections – ASIO responded to third-party information disclosure requests in criminal prosecutions
- involvement in other civil law matters and proceedings, including regarding the protection of sensitive information in that context
- involvement in, and provision of, information to assist in inquisitorial matters, including a coronial inquest and a judicial inquiry
- involvement in applications for post-sentence orders that have used ASIO information.

Federal Court of Australia and High Court of Australia proceedings

ASIO was involved in proceedings in the Federal Court of Australia and the High Court of Australia. This included matters where the Director-General of Security was a respondent (such as judicial review proceedings relating to security assessment decisions). In these matters, ASIO worked closely with other stakeholders to manage the collective Commonwealth interest, including ensuring that sensitive information received appropriate protections throughout the proceedings.

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 and other highly paid staff remuneration is discussed at **Appendix E**.

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

Performance management

Maintaining a high-performing workforce ensures ASIO can fulfil its purpose. The *ASIO Performance Management Framework* supports the development of the skills and capability required to achieve the Organisation's strategic and operational goals, and the ongoing development of ASIO's employees.

Consistent with policy requirements, all ASIO employees participated in the 2024–25 Performance Management Cycle.

ASIO's performance management framework supports employee development, talent management and includes the future learning objectives and goals for ASIO employees. The performance framework includes toolkits for all employees to take ownership for their own career, both in their day-to-day roles as well as their long-term aspirations. This includes ASIO's commitment to diversity, inclusion and mentoring. The performance process also underpins ASIO's retention plan, and ensures that leaders and employees are aligned in career conversations.

ASIO is committed to the development and support of its leaders through its Manager-Once-Removed Feedback mechanism which is incorporated into ongoing performance and career conversations. ASIO also has a well-established talent management framework for its Senior Executive Service (SES) employees to ensure continued alignment with the Australian Public Service Commission (APSC) framework, and SES performance agreements have been updated to include the APSC focus on performance and behaviour. This year ASIO commenced a new talent management process for its EL2 and EL3 employees to support stronger succession and career management.

Diversity and inclusion

Diversity and inclusion are critical components of our organisational success. To effectively deliver our mission, we require a workforce that reflects the diverse Australian community we protect. A diverse range of experiences, skills and abilities enables us to approach problems from multiple angles, driving innovation and informed decision-making. Furthermore, we know that a positive and inclusive work environment fosters creativity and innovation, and improves productivity, which in turn improves employee satisfaction and retention. Our people are our most important asset and we are committed to inclusion, focusing on creating an environment where all employees feel valued, respected and supported.

ASIO is committed to ensuring its workforce reflects the diversity of Australian society. To achieve this, diversity is at the forefront of our recruitment strategies, which have included affirmative measures such as Indigenous and disability-focused rounds.

Our commitment to diversity and inclusion is guided by our diversity and inclusion strategy. Following the completion of the *ASIO Diversity and Inclusion Strategy 2021–24*, work has been underway on the development of ASIO's diversity and inclusion strategy 2025-28. This will be the roadmap for prioritising action and monitoring progress towards our diversity and inclusion objectives over the next 3 years.

We have made significant strides in creating a more inclusive environment for our employees, particularly through the dedication of our staff-led diversity networks. These 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 quarterly reporting of network outcomes.

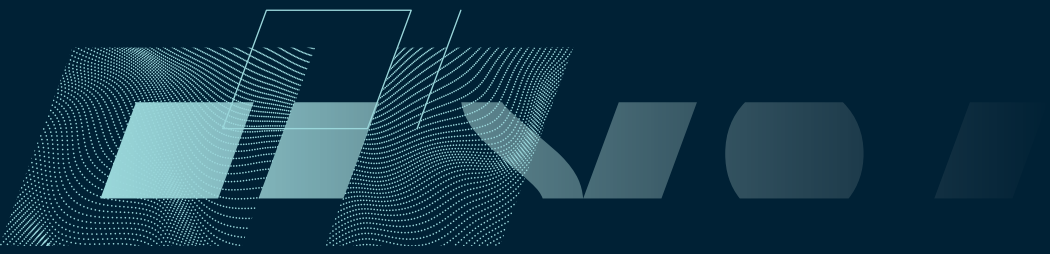
Some notable achievements include:

- Through the ASIOpen network, we have achieved Gold-level recognition in the Australian Workplace Equality Index for the second year running. ASIO is one of only 7 public sector employers to do so and the first NIC agency to achieve this status.
- We have established a Neurodiversity Working Group to raise awareness and educate staff on working with neurodivergent individuals, and provide guidance to managers and teams to better support them.
- We remain committed to our *Disability Action Plan 2022–24*, with ongoing efforts to foster a culture of inclusivity and provide effective support for all staff. Building on our progress, a new plan for 2025 and beyond has begun, ensuring our continued focus on disability inclusion and support.

- We continue to acknowledge and celebrate the important contributions of Aboriginal and Torres Strait Islander culture in our workplace and in Australian society, through activities such as National Reconciliation Week and NAIDOC Week. Additionally, we attended the second Five Eyes Indigenous conference in Canada, which connected Australian and Five Eyes networks and identified areas for future collaboration and learning.

ASIO is compliant with the reporting obligations of the *Workplace Gender Equality Act 2012*. Statistics on the diversity of our workforce are provided at **Appendix G** and **Appendix S**.[7]

[7] Consistent with the determination issued to ASIO by the Minister of Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, detailed statistics on workforce diversity have been deleted from the version of the *ASIO Annual Report 2024–25* tabled in parliament (**Appendix S**).



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 LGBTQIA+ network promotes an inclusive workplace culture and supports lesbian, gay, bisexual, transgender, queer, intersex, asexual and other sex, gender and sexually diverse individuals to be open and authentic in the workplace and reach their full potential. ASIOpen celebrates the benefits of inclusivity, builds a sense of belonging, and drives reform on issues relating to sex, gender and sexually diverse employees and families. This is achieved through information sharing, hosted events and policy reform.

Ability

Our Ability network represents staff experiencing all forms of physical and mental health issues, neurodiversity and caring responsibilities. Ability advocates for increased awareness, acceptance and respect for all forms of ability within ASIO. Ability 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 Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to all Aboriginal and Torres Strait Islander peoples, their cultures and to their Elders past and present. 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 First Nations peoples.

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.

Other mandatory information

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 audit of ASIO's roles and activities has been undertaken to ensure that existing and emerging risks to children are identified and that appropriate mitigation strategies are developed. While the assessed likelihood of risks to children occurring is rare, the overall risk rating of the safety of children and young people as at 30 June 2025 is assessed as medium.

ASIO's activities are consistent with each of the 4 requirements of the Commonwealth Child Safe Framework. 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, there are strong safeguards embedded in legislation relating to the compulsory questioning of minors under the ASIO Act. Staff are aware of the sensitivities that apply when working with children and have access to specialist advice as required.

All of ASIO's activities are subject to oversight by the Inspector-General of Intelligence and Security, who is responsible for reviewing the activities of intelligence agencies for legality, propriety and consistency with human rights.

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

We will continue to review child-related risks where relevant to further refine policies and procedures, and improve staff awareness.

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.

Statistics on the diversity of our workforce, including statistics on people with disability, are provided at **Appendix G** and **Appendix S**.[8]

[8] Consistent with the determination issued to ASIO by the Minister of Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, detailed statistics on workforce diversity have been deleted from the version of the *ASIO Annual Report 2024–25* tabled in parliament (**Appendix S**).

Work Health and Safety Act 2011

Schedule 2, part 4 of the *Work Health and Safety Act 2011* requires non-corporate Commonwealth entities to include in their annual report information on health and safety outcomes and initiatives taken during the reporting period to ensure the health, safety and welfare of workers who carry out work for them. Our report for 2024–25 is provided at **Appendix H**.

Recruitment, advertising and market research

ASIO needs talented people who are highly capable, dedicated, adaptable and resilient. We seek to reflect the diversity of the community we protect, and continue to develop and implement attraction strategies to achieve this.

In the 2024–25 financial year, ASIO expended $454,541 on advertising and marketing for recruitment activities and campaigns.

During the reporting year, we continued to adapt and refine our approach to recruitment in order to remain an employer of choice for Australia's best and brightest. We focused on growing our own capability through entry-level roles in intelligence, technology, strategic policy, governance and communications, legal, HR, finance, vetting and traineeships. ASIO undertook targeted recruitment to fill critical capabilities with specialist skills in technology, project management, business analysis and corporate services.

ASIO had nil expenditure on other types of advertising and market research during 2024–25.

Purchasing

During 2024–25 ASIO adhered to the Commonwealth Procurement Rules (CPR) and associated policy and guidelines. ASIO's compliance was monitored by the Audit and Risk Committee. No significant issues were identified and overall compliance was acceptable.

Annual reports contain information about actual expenditure on reportable consultancy and non-consultancy contracts. Information on the value of reportable consultancy and non-consultancy contracts is available on the AusTender website. However, ASIO is not required to publish information on the AusTender website, in line with exemptions for protection of essential security interests. A list of consultancy and non-consultancy contacts 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 followed internal policy and associated procedures on identifying and determining the nature of a contract. This ensured that we used appropriate methods for engaging and contracting consultants.

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

As shown in Table 1, in 2024–25, 64 new consultancy contracts were entered into involving total actual expenditure of $8.55 million. In addition, 15 ongoing consultancy contracts were active during the period, with total actual expenditure of $3.31 million.

Non-consultancies

As shown in Table 2, in 2024–25, 553 new non-consultancy contracts were entered into with total actual expenditure of $93.30 million. In addition, 414 ongoing non-consultancy contracts were active during the reporting period, with total actual expenditure of $176.91 million.

Table 1: Expenditure on reportable consultancy contracts current reporting period (2024–25)

	Number	Expenditure $'000 (GST inc.)
New contracts entered into during the reporting period	64	8,550
Ongoing contracts entered into during a previous reporting period	15	3,308
Total	**79**	**11,858**

Table 2: Expenditure on reportable non-consultancy contracts current reporting period (2024–25)

	Number	Expenditure $'000 (GST inc.)
New contracts entered into during the reporting period	553	93,303
Ongoing contracts entered into during a previous reporting period	414	176,908
Total	**967**	**270,211**

Australian National Audit Office access clauses

During the 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 of Security has applied measures necessary for the protection of essential security interests in accordance with clause 2.6 of the CPR, which exempts ASIO from publishing details of contract arrangements, including standing offers on AusTender.

Details of our arrangements, contracts and standing offers are available to the PJCIS 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
- 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 the Australian Government Payments to Small Business are available on the Treasury's website.

Asset management

The Organisation's governance framework to provide assurance that asset balances in the financial statements are accurately reported includes:

- asset investment and replacement program, based on: 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 and priorities.
- 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 3-yearly revaluations of all tangible assets, which is completed by qualified external valuers. A materiality review is undertaken in the years in between valuations
- maintaining property, plant and equipment assets through maintenance programs
- providing a centralised procurement policy and advice service, including quality control oversight.

APS Net Zero 2030 Policy

APS Net Zero 2030 is the government's policy for the APS to reduce its greenhouse gas emissions to net zero by 2030, and transparently report on its emissions from the latter half of 2023. Our public reporting of greenhouse gas emissions inventory for 2024–25 is provided at **Appendix I**.

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 2024–25 is provided at **Appendix I**.

Commonwealth Climate Disclosure Policy

Commonwealth Climate Disclosure (CCD) is the government's policy for Commonwealth entities to publicly report on their exposure to climate risks and opportunities, as well as their actions to manage them, delivering transparent and consistent climate disclosures to the Australian public.

We have provided data against CCD criteria pertaining to gross greenhouse gas emissions generated during the reporting period at **Appendix I**. We have not provided information on the processes, controls and procedures we use to monitor, manage and oversee our climate-related risks and opportunities, given operational sensitivities.

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; 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 the use of technical assistance requests, technical assistance notices and technical capability notices, **Appendix O** relating to the 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, the PJCIS, IGIS, INSLM and the Leader of the Opposition.





5

FINANCIAL INFORMATION

Financial information

ASIO prepared financial statements for the year ended 30 June 2025 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) which has 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 2024–25*.

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 determination issued under section 105D of the PGPA Act.

CONTENTS

STATEMENT OF COMPREHENSIVE INCOME 75

STATEMENT OF FINANCIAL POSITION 76

STATEMENT OF CHANGES IN EQUITY 77

STATEMENT OF CASH FLOWS 78

NOTES TO THE FINANCIAL INFORMATION 79

1. Financial performance 80

1.1 EXPENSES 80

1.2 OWN-SOURCE REVENUE 80

1.3 REVENUE FROM GOVERNMENT 80

2. Financial position 81

2.1 FINANCIAL ASSETS 81

2.2 NON-FINANCIAL ASSETS 81

2.3 PAYABLES 83

2.4 INTEREST BEARING LIABILITIES 83

2.5 PROVISIONS 83

3. Funding 84

3.1 APPROPRIATIONS 84

4. Managing uncertainties 85

4.1 CONTINGENT ASSETS AND LIABILITIES 85

4.2 FINANCIAL INSTRUMENTS 85

5. Other information 86

5.1 CURRENT/NON-CURRENT DISTINCTION FOR ASSETS AND LIABILITIES 86

5.2 KEY MANAGEMENT PERSONNEL REMUNERATION 86

5.3 RELATED PARTY DISCLOSURES 87

5.4 MAJOR BUDGET VARIANCES 88

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2025

	Notes	2025 $'000	Original budget 2025 $'000	2024 $'000
EXPENSES	1.1	732,721	729,462	666,929
OWN-SOURCE INCOME	1.2			
Revenue		23,456	20,833	18,511
Gains		6,163	165	2,873
Net cost of services		***(703,102)***	***(708,464)***	***(645,545)***
REVENUE FROM GOVERNMENT		**598,587**	**594,277**	**534,082**
DEFICIT ON CONTINUING OPERATIONS		**(104,515)**	**(114,187)**	**(111,463)**
OTHER COMPREHENSIVE INCOME		9,979	-	(3,765)
TOTAL COMPREHENSIVE LOSS		**(94,536)**	**(114,187)**	**(115,228)**

STATEMENT OF FINANCIAL POSITION as at 30 June 2025

	Notes	2025 $'000	Original budget 2025 $'000	2024 $'000
ASSETS				
Financial assets	2.1	307,628	199,114	262,968
Non-financial assets	2.2	930,476	946,503	893,910
TOTAL ASSETS		**1,238,104**	**1,145,617**	**1,156,878**
LIABILITIES				
Payables	2.3	110,898	55,628	63,748
Interest bearing liabilities	2.4	533,915	497,122	556,105
Provisions	2.5	124,108	116,090	109,623
TOTAL LIABILITIES		**768,921**	**668,840**	**729,476**
NET ASSETS		**469,183**	**476,777**	**427,402**
EQUITY				
Parent equity interest				
Contributed equity		1,475,345	1,496,942	1,339,028
Reserves		146,049	139,835	136,070
Accumulated deficit		(1,152,211)	(1,160,000)	(1,047,696)
TOTAL EQUITY		**469,183**	**476,777**	**427,402**

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2025

	2025 $'000	Original budget 2025 $'000	2024 $'000
RETAINED EARNINGS			
Opening balance	(1,047,696)	(1,045,813)	(936,233)
Comprehensive income			
Deficit for the period	(104,515)	(114,187)	(111,463)
Closing balance	***(1,152,211)***	***(1,160,000)***	**(1,047,696)**
ASSET REVALUATION RESERVE			
Opening balance	136,070	139,835	139,835
Other comprehensive income	9,979	-	(3,765)
Closing balance	***146,049***	***139,835***	**136,070**
CONTRIBUTED EQUITY			
Opening balance	1,339,028	1,346,433	1,211,498
Transactions with owners			
Contributions by owners			
Equity injection – appropriation	86,161	87,053	63,705
Departmental capital budget	50,156	63,456	63,825
Closing balance	***1,475,345***	***1,496,942***	**1,339,028**
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	**469,183**	**476,777**	**427,402**

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
as at 30 June 2025

	2025 $'000	Original budget 2025 $'000	2024 $'000
OPERATING ACTIVITIES			
Cash received			
Appropriations	652,925	619,208	600,343
Other	55,844	42,032	51,754
Cash used	662,990	620,481	635,501
NET CASH FROM/(USED BY) OPERATING ACTIVITIES	**45,779**	**40,759**	**16,596**
INVESTING ACTIVITIES			
Cash received	1,088	-	767
Cash used	164,879	169,889	107,192
NET CASH FROM/(USED BY) INVESTING ACTIVITIES	**(163,791)**	**(169,889)**	**(106,425)**
FINANCING ACTIVITIES			
Cash received	163,460	169,889	102,224
Cash used	38,204	40,567	40,526
NET CASH FROM/(USED BY) FINANCING ACTIVITIES	**125,256**	**129,322**	**61,698**
Net increase (decrease) in cash held	7,244	192	(28,131)
Cash and cash equivalents at the beginning of the reporting period	26,836	57,783	54,967
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD	**34,080**	**57,975**	**26,836**

NOTES TO THE FINANCIAL INFORMATION

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 including simplified disclosures for Tier 2 Entities under AASB 1060 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 issued prior to the signing of the statement by the Director-General that are applicable to the current reporting period.

Taxation

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

Events after the reporting period

Additional property-related arrangements commenced from July 2025 which will result in an increase to the Lease Liability.

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.

1.3 REVENUE FROM GOVERNMENT

Accounting policy

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

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 (2024: 30 days).

Financial assets were assessed for impairment at 30 June 2025. 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 on acquisition except as stated below. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken. Financial assets are initially measured at their fair value plus transaction costs where appropriate.

Purchases of non-financial assets are initially recognised at cost in the statement of financial position, except for purchases costing less than $4,000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

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 2025. 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 May 2025. A desktop revaluation of the Leasehold asset class was undertaken with adjustments made on a class basis. The valuer has provided written assurance to ASIO that the models developed are in compliance with AASB 13 Fair Value Measurement.

The market approach has been utilised to determine the fair value of identified land, buildings, plant and equipment. The market approach considered transactions and pricing data that has occurred in the principal market in arriving at fair value. The Depreciated Replacement Cost (DRC) approach has been utilised to determine fair value. The DRC approach reflects the amount a market participant will be prepared to pay to acquire or construct a substitute asset of comparable utility, adjusted for physical depreciation and obsolescence.

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 materiality review 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 2023.

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	Capital budget	Equity injections
	$'000	$'000	$'000
2025			
Appropriation Act			
Annual appropriation	598,587	63,456	87,153
PGPA Act			
Section 74 transfers	110,385	-	-
Total appropriation	**708,972**	**63,456**	**87,153**
Appropriation applied (current and prior years)	(645,123)	(54,620)	(108,841)
Variance	***63,849***	***8,836***	***(21,688)***
2024			
Appropriation Act			
Annual appropriation	534,082	63,825	71,442
PGPA Act			
Section 74 transfers	94,968	-	-
Total appropriation	**629,050**	**63,825**	**71,442**
Appropriation applied (current and prior years)	(625,847)	(52,584)	(49,640)
Variance	***3,203***	***11,241***	***21,802***

4. Managing uncertainties

4.1 CONTINGENT ASSETS AND LIABILITIES

Quantifiable contingencies

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

Unquantifiable contingencies

At 30 June 2025, 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

	2025 $'000	2024 $'000
5.1 CURRENT/NON-CURRENT DISTINCTION FOR ASSETS AND LIABILITIES		
Assets expected to be recovered in:		
No more than 12 months	334,629	289,545
More than 12 months	903,475	867,333
Total assets	**1,238,104**	**1,156,878**
Liabilities expected to be recovered in:		
No more than 12 months	187,652	133,564
More than 12 months	581,269	595,912
Total liabilities	**768,921**	**729,476**

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	2,733	2,510
Long-term employee benefits	119	121
Post-employment benefits	446	413
Total key management personnel remuneration expenses	**3,298**	**3,044**

The number of key management positions as at 30 June 2025 is 6 (2024: 6).

Membership of the Executive Committee changed throughout 2024–25 with an officer retiring and a new officer joining.

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 2024–25 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 2024–25 Portfolio Budget Statements (PBS) and the 2024–25 actual result. The budget is not audited. Where the published budget is not disaggregated to the financial statements level, budget figures are derived from internal documentation used in developing the budget. 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 2024–25 Budget PBS may be amended by Government throughout the year.

Expenses

Total expenses is $3.259 million (0.5%) greater than original budget. Operating costs reflect the impact of a competitive workplace market and inflationary pressures on supply chains.

Income

Total own-sourced-income is $8.621 million (41%) greater than original budget. This budget is dependent on requests and activities undertaken by external parties which was greater than anticipated, and an increase in gains was recognised.

Assets

Total assets is $78.255 million (7%) greater than original budget due to an increase in trade and other receivables, which is offset by fewer non-financial asset purchases.

Liabilities

Total liabilities is $85.849 million (13%) greater than original budget. The variance is largely due to inflationary increases, and changes in provisions and liabilities.

Statement of changes in equity

Total equity is $7.594 million (2%) lower than budget due to reduced deficit, an increase in the asset revaluation reserve, and section 51 quarantines within contributed equity.

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.





A
APPENDICES

Appendix A: ASIO resource statement

	Actual available appropriation 2025 $'000	Payments made 2025 $'000	Balance remaining 2025 $'000
Departmental			
Annual appropriations – ordinary annual services[1]			
Prior year appropriation[2]	152,148	138,848	13,300
Departmental appropriation[3]	598,587	427,233	171,354
s74 external revenue[4]	110,385	110,385	-
Departmental capital budget[5]	63,456	31,078	32,378
Cash on hand	26,836	(7,244)	34,080
Annual appropriations – other services – non-operating[6]			
Prior year appropriation[7]	64,373	55,644	8,729
Equity injections	87,153	53,197	33,956
Total net resourcing and payments for ASIO	**1,102,938**	**809,141**	**293,797**

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

2 Includes $13.300 million that was withheld under section 51 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

3 Excludes departmental capital budget (DCB).

4 External receipts under section 74 of the PGPA Act.

5 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'.

6 Appropriation Act (No.2) and Appropriation Act (No.4).

7 Includes $8.729 million that was withheld under section 51 of the PGPA Act.

Due to rounding, figures presented may not add precisely to the totals provided.

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] 2025 $'000	Actual expenses 2025 $'000	Variation 2025 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Departmental appropriation	598,587	490,521	108,066
s74 external revenue[2]	21,240	110,385	(89,145)
Expenses not requiring appropriation in the budget year[3]	128,522	131,815	(3,293)
Total for Program 1.1	***748,349***	***732,721***	***15,628***
Total expenses for Outcome 1	**748,349**	**732,721**	**15,628**

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

2 Estimated expenses incurred in relation to receipts retained under section 74 of the PGPA Act.

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 Philip Moss AM was appointed as the Independent Reviewer for a term of three years commencing on 17 January 2022. This term of appointment was extended until 10 July 2025.

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 ASA, 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.

New matters arising during the year

No new matters were referred to the Independent Reviewer during 2024–25.

Philip Moss AM

Independent Reviewer of
Adverse Security Assessments

Appendix D: report of the Independent Reviewer of Security Clearance Decisions

Appointment of the Independent Reviewer of Security Clearance Decisions

Mr Philip Moss AM was appointed the Independent Reviewer for a term of 18 months commencing on 10 January 2024.

The role of the Independent Reviewer

The Independent Reviewer's role is to review certain security clearance decisions for persons who did not hold an existing security clearance nor were Commonwealth employees immediately before the original security clearance decision was made.

Independently reviewable decisions are decisions, made following internal review, to:

- deny a security clearance,
- revoke a security clearance, or
- impose or vary a condition on a security clearance.

ASIO must provide the affected person with notice of their right to apply for independent review.

When the Independent Reviewer receives a written request for review from an affected person, they must decide, as soon as practicable after receiving the application, whether they will review the decision.

Should the Independent Reviewer decide to review the decision, the Independent Reviewer must review the decision in as timely a manner as possible, and in their review they must consider all the information provided to them by the Director-General of Security.

Once the Independent Reviewer has completed a review, they must provide to the Director-General of Security and the Inspector-General of Intelligence and Security, their opinion as to whether the decision was reasonably open to have been made.

Within 14 days of providing the opinion to the Director-General of Security, the Independent Reviewer must give the affected person and the sponsoring agency of the security clearance notice that the opinion has been given. The Independent Reviewer must not give the affected person and the sponsoring agency the opinion.

New matters arising during the year

During the period ending 30 June 2025 no matters were referred to the Independent Reviewer.

Philip Moss AM

Independent Reviewer of Security Clearance Decisions

Appendix E: executive remuneration

Key management personnel remuneration

Categories of ASIO's key management personnel include:

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

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 Relations Policy 2023*.

The following tables show the remuneration of key management personnel, senior executives and other highly paid staff in 2024–25 in accordance with the Public Governance, Performance and Accountability Rule 2014.

Information about remuneration for key management personnel

			Short-term benefits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration[3]
Name	Term	Position title	Base salary[1] $	Bonuses $	Other benefits and allowances $	Superannuation contributions $	Long service leave[2] $	Other long-term benefits $	$	$
Mike BURGESS	01 Jul 24 – 30 Jun 25	Director-General[4]	659,587	0	0	98,338	15,023	0	0	772,948
Mike NOYES	01 Jul 24 – 30 Jun 25	Deputy Director-General	435,210	0	0	73,758	38,649	0	0	547,617
Lisa ALONSO LOVE	18 Nov 24 – 30 Jun 25	Deputy Director-General	290,231	0	0	53,541	28,186	0	0	371,958
Hazel BENNETT	01 Jul 24 – 22 Nov 24	Deputy Director-General	187,215	0	0	33,586	4,449	0	0	225,250
Peter (Gus) GILMORE	01 Jul 24 – 30 Jun 25	Deputy Director-General	417,271	0	0	56,899	8,925	0	0	483,095
Name withheld[5]	01 Jul 24 – 30 Jun 25	Principal Advisor	406,808	0	0	67,715	8,705	0	0	483,228
Name withheld[5]	01 Jul 24 – 30 Jun 25	General Counsel	336,948	0	0	62,223	14,796	0	0	413,967

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*. Discount rate variations throughout the year will affect the value.

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

4 The pro-rata remuneration in this table differs from that shown in *Remuneration Tribunal (Remuneration and Allowances for Holders of Full-time Public Office) Determination 2024* 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 annual and long service leave, and superannuation.

5 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

			Short-term benefits		Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration[3]
Remuneration bands	Number of senior executives	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 $	Average total remuneration $
$0 to $220,000	20	82,430	0	287	12,600	1,747	0	0	97,064
$220,001 to $245,000	1	198,482	0	0	22,744	504	0	0	221,730
$245,001 to $270,000	3	204,553	0	0	33,077	18,732	0	0	256,362
$270,001 to $295,000	3	230,043	0	0	39,031	16,982	0	0	286,056
$295,001 to $320,000	14	256,464	0	2,182	42,520	7,825	0	0	308,991
$320,001 to $345,000	12	266,836	0	748	45,615	17,238	0	0	330,437
$370,001 to $395,000	6	306,547	0	0	48,722	31,152	0	0	386,421
$395,001 to $420,000	7	304,776	0	42	45,827	21,361	0	34,249	406,255
$420,001 to $445,000	1	330,332	0	0	55,397	35,392	0	0	421,121
$470,001 to $495,000	2	338,353	0	6,437	53,217	84,519	0	0	482,526
$495,001 to $520,000	2	364,165	0	1,062	47,698	91,791	0	0	504,716
$520,001 to $545,000	1	153,687	0	430	28,409	3,981	0	337,794	524,301
$545,001 to $570,000	1	502,970	0	0	57,445	-3,171	0	0	557,244

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*. Discount rate variations throughout the year will affect the value.

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

Information about remuneration for other highly paid staff

		Short-term benefits		Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration[3]
Remuneration bands	Number of highly paid staff	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 $	Average total remuneration $
$260,000 to $270,000	18	214,372	0	6,861	30,666	12,279	0	0	264,178
$270,001 to $295,000	28	225,006	0	6,348	34,573	15,503	0	0	281,430
$295,001 to $320,000	19	250,905	0	8,294	32,452	12,973	0	0	304,624
$320,001 to $345,000	6	260,372	0	33,692	32,520	4,795	0	0	331,379
$345,001 to $370,000	3	309,995	0	795	29,056	11,880	0	0	351,726
$370,001 to $395,000	5	296,245	0	2,048	25,519	6,173	0	50,590	380,575
$395,001 to $420,000	2	256,995	0	2,101	25,210	5,326	0	121,924	411,556
$445,001 to $470,000	1	413,782	0	0	33,363	6,011	0	0	453,156
$495,001 to $520,000	1	140,568	1	0	49,890	3,552	1	320,269	514,281

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*. Discount rate variations throughout the year will affect the value.

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

Appendix F: ASIO's salary classification structure

Senior Executive Service	Minimum salary	Maximum salary
SES 3	402,561	
SES 2	319,280	
SES 1	260,557	
Senior employees		
AEE 3	215,202	
AEE 2	156,365	185,029
AEE 1	136,428	152,454
Employees		
AE 6	107,346	120,947
AE 5	97,122	104,249
AE 4	88,512	94,964
AE 3	78,276	85,529
AE 2	68,841	76,257
AE 1	59,430	66,010

Note: Figures are as applied in 2024–25 and exclude Individual Flexibility 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 G: workforce statistics[1]

Statistics for ongoing employees by gender – current reporting period (2024–25) percentage of total workforce

	Man/Male			Woman/Female			Non-binary			Prefers not to answer			Uses a different term		
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total non-binary**	Full-time	Part-time	**Total prefers not to answer**	Full-time	Part-time	**Total uses a different term**
Total	**50.8%**	**2.7%**	**53.5%**	**37.3%**	**8.7%**	**45.9%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.1%**	**0.0%**	**0.1%**

Statistics for non-ongoing employees by gender – current reporting period (2024–25) percentage of total workforce

	Man/Male			Woman/Female			Non-binary			Prefers not to answer			Uses a different term		
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total non-binary**	Full-time	Part-time	**Total prefers not to answer**	Full-time	Part-time	**Total uses a different term**
Total	**0.3%**	**0.1%**	**0.4%**	**0.1%**	**0.0%**	**0.1%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**

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

[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*, ASIO workforce statistics by headcount have been deleted from the version of the *ASIO Annual Report 2024–25* tabled in parliament (**Appendix S**).

Statistics for ongoing employees by gender – previous reporting period (2023–24) percentage of total workforce

	Man/Male			Woman/Female			Non-binary			Prefers not to answer			Uses a different term		
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total non-binary**	Full-time	Part-time	**Total prefers not to answer**	Full-time	Part-time	**Total uses a different term**
Total	**50.3%**	**2.5%**	**52.7%**	**37.3%**	**9.2%**	**46.4%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.1%**	**0.0%**	**0.1%**

Statistics for non-ongoing employees by gender – previous reporting period (2023–24) percentage of total workforce

	Man/Male			Woman/Female			Non-binary			Prefers not to answer			Uses a different term		
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total non-binary**	Full-time	Part-time	**Total prefers not to answer**	Full-time	Part-time	**Total uses a different term**
Total	**0.1%**	**0.5%**	**0.6%**	**0.0%**	**0.2%**	**0.2%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**

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

Statistics on full-time and part-time employees – current reporting period (2024–25) percentage of total workforce

	Ongoing			Non-ongoing		
	Full-time	Part-time	**Total ongoing**	Full-time	Part-time	**Total non-ongoing**
Total	**88.1%**	**11.4%**	**99.5%**	**0.4%**	**0.1%**	**0.5%**

Statistics on full-time and part-time employees – previous reporting period (2023–24) percentage of total workforce

	Ongoing			Non-ongoing		
	Full-time	Part-time	**Total ongoing**	Full-time	Part-time	**Total non-ongoing**
Total	**87.6%**	**11.8%**	**99.3%**	**0.1%**	**0.6%**	**0.7%**

Employment type by location – current reporting period (2024–25) percentage of total workforce

	Ongoing	**Non-ongoing**
All locations	99.5%	0.5%
Total	**99.5%**	**0.5%**

Employment type by location – previous reporting period (2023–24) percentage of total workforce

	Ongoing	**Non-ongoing**
All locations	99.3%	0.7%
Total	**99.3%**	**0.7%**

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

People with disability employment – current reporting period (2024–25) percentage of total workforce

Ongoing	2.2%
Non-ongoing	0.1%
Total	**2.2%**

People with disability employment – previous reporting period (2023–24) percentage of total workforce

Ongoing	1.9%
Non-ongoing	0.0%
Total	**1.9%**

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

Appendix H: work health and safety

ASIO is committed to providing a safe work environment for all staff. Our safety management system includes strategies to identify emerging risks, respond to hazards and support ill or injured staff.

Across a diverse range of workplaces and work activities, safety risks are proactively assessed and managed, reducing the risk associated with serious workplace injury. Staff are encouraged to raise and report workplace safety concerns whether physical or psychosocial. By actively addressing workplace safety risks, ASIO demonstrates a focus on continuous improvement and is well-placed in terms of legislative compliance.

Safety leadership

ASIO recognises the importance of leadership in safety. We're supporting managers to increase engagement on safety issues within their teams and build a positive safety culture. Managers are provided with tools and resources to take ownership of safety risks and to develop appropriate controls. Managers are uniquely placed to understand, in detail, work activities and requirements and can effectively mitigate risks as required.

Targeted training for managers on their work health and safety obligations, including personal responsibilities and due diligence requirements has increased awareness and understanding around the importance of rigorous workplace safety procedures.

Psychosocial safety and wellbeing

ASIO continues to invest in mental health literacy, in particular, awareness of the key workplace psychosocial factors and the potential for harm. Training and resources are aimed at avoiding challenges as a result of psychosocial hazards, providing staff with guidance and support to navigate and mitigate these issues.

ASIO's health and wellbeing program continues to support the workforce through a range of services and programs, including:

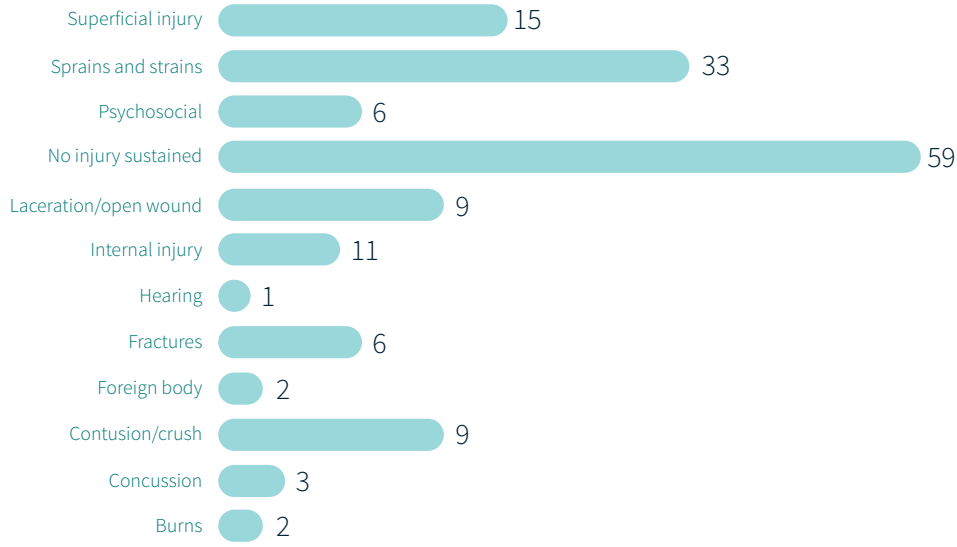
- annual workplace influenza vaccinations
- Employee Assistance Program and other psychological support services
- Early Intervention Program
- assistance with accommodating reasonable workplace adjustments
- ergonomic/sedentary risk services
- promotion of physical and psychological health.

Incidents

In accordance with legislated notification obligations, ASIO reported 6 incidents to Comcare in 2024–25. In consultation with Comcare, each of the incidents was investigated by ASIO to ensure appropriate controls and prevention strategies are implemented. No notices were issued to ASIO by Comcare.

Staff are encouraged to report both physical and psychosocial issues. In the 2024–25 period, 6 workplace psychosocial incidents were reported, relating in particular to workplace stress and the impact of change in the workplace.

The following table outlines safety incidents by mechanism of injury for the period 2024–25.



Appendix I: climate statement

ASIO uses governance and risk management policies, procedures and tools to manage our climate-related risks and opportunities. We are committed to climate action, including playing our part in achieving the APS Net Zero Emissions by 2030 commitment and reporting on our progress through climate disclosures – where these do not reveal operational sensitivities – in our annual reports.

To the greatest extent possible, ASIO undertakes its property functions in a sustainable manner. ASIO constantly looks for ways to optimise practices and processes.

Emissions reporting/climate-related metrics

As part of the *Net Zero in Government Operations Strategy*, and the reporting requirements under section 516A of the *Environment Protection and Biodiversity Conservation Act 1999*, Commonwealth entities are required to report on their operational greenhouse gas emissions.

The Greenhouse Gas Emissions Inventory table presents greenhouse gas emissions over the 2024–25 financial year. The greenhouse gas emissions reported are calculated on the basis of carbon dioxide equivalent (CO_2-e) and in line with the Emissions Reporting Framework. This is consistent with a whole-of-Australian Government approach, outlined in the *Net Zero in Government Operations Strategy*, and *Commonwealth Climate Disclosure* requirements.

2024–25 Greenhouse Gas Emissions Inventory – location-based method

Emission source	Scope 1 t CO_2-e	Scope 2 t CO_2-e	Scope 3 t CO_2-e	Total t CO_2-e
Electricity (location-based approach)	N/A	14,085.78	853.68	14,939.46
Natural gas	698.39	N/A	177.55	875.93
Solid waste	–	N/A	122.40	122.40
Refrigerants[1]	356.93	N/A	N/A	356.93
Fleet and other vehicles[2]	–	N/A	–	–
Domestic commercial flights[2]	N/A	N/A	–	–
Domestic hire car[2]	N/A	N/A	–	–
Domestic travel accommodation[2]	N/A	N/A	–	–
Other energy	49.75	N/A	12.26	62.01
Total t CO_2-e	**1,105.07**	**14,085.78**	**1,165.89**	**16,356.73**

Note: The table above presents emissions related to electricity usage using the location-based accounting method.

Key: CO_2-e = carbon dioxide equivalent; N/A = not applicable

[1] ASIO is reporting refrigerant emissions for the first time in 2024–25, having opted to include them in alignment with the Emissions Reporting Framework. While reporting of refrigerant emissions was optional in 2023–24, ASIO has adopted the prescribed methodology to quantify and disclose these emissions in the current reporting period.

[2] This sensitive data was not included.

Sustainability report

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.

Energy efficiency

Priorities

- Continue to replace LED lights to reduce use of fluorescent and metal halide lights
- Further optimise efficiency of air-conditioning system to reduce demand on boilers, chillers and cooling towers
- Maintain Ben Chifley Building's energy-producing infrastructure to optimise behind-the-meter renewable energy production and consumption

Actions

- Continued working on our energy efficiency priorities
- Participated in national environmental events such as Earth Hour
- Used ICT equipment with built-in energy-saving features to enter low power states when not in use

Waste

Priorities

- Investigate other recycling options to reduce waste to landfill

Actions

- Recycled waste including batteries, cardboard, coffee beans, coffee cups, co-mingled waste, cooking oil, e-waste, fluorescent lights, food waste, grease-trap waste, green waste, paper, polystyrene, scrap metal, toner cartridges and wooden pallets

Water

Priorities

- Optimise water use

Actions

- Planned water-sparing gardens to replace end-of-life gardens
- Used captured stormwater for irrigation and toilet flushing to reduce reliance on potable water

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.

Subsection	Description	2022–23	2023–24	2024–25
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	0	0
94(1)(b)	The total number of warrants issued during the period under that Division (including the number of warrants issued orally)	0	0	0
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	0	0	0
Total hours		**0**	**0**	**0**
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	0	0	0

Appendix K: correction of material errors in previous annual reports

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

An error has been identified in **Appendix M** of the *ASIO Annual Report 2023–24* regarding statistics required under section 94 of the ASIO Act relating to requests for access to data under the *Telecommunications (Interception and Access) Act 1979*. A correction is provided in **Appendix M** to the *ASIO Annual Report 2024–25*.



P

PRELIMINARIES



List of annual report requirements under schedule 2 of the PGPA 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	Preliminaries
17AJ(c)	Glossary of abbreviations and acronyms.	Mandatory	Preliminaries
17AJ(d)	List of requirements.	Mandatory	Preliminaries
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 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

PGPA Rule reference	Description	Requirement	Part of this report
17AE(1)(a)(ii)	A description of the organisational structure of the entity.	Mandatory	Part 2 and Appendix U
17AE(1)(a)(iii)	A description of the outcomes and programmes administered by the entity.	Mandatory	Part 2
17AE(1)(a)(iv)	A description of the purposes of the entity as included in corporate plan.	Mandatory	Part 2
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.	If applicable, Mandatory	Not applicable
17AD(c)	**Report on the Performance of the entity**		
	Annual performance Statements		
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 3 and Appendix T
17AD(c)(ii)	***Report on Financial Performance***		
17AF(1)(a)	A discussion and analysis of the entity's financial performance.	Mandatory	Part 3 Part 5 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.	If applicable, Mandatory	Not applicable

PGPA Rule reference	Description	Requirement	Part of this report
17AD(d)	**Management and Accountability**		
	Corporate Governance		
17AG(2)(a)	Information on compliance with section 10 (fraud systems).	Mandatory	Letter of transmittal and Part 4
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 4
17AG(2)(d) – (e)	A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to non-compliance with Finance law and action taken to remedy non-compliance.	If applicable, Mandatory	Not applicable
	Audit Committee		
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

PGPA Rule reference	Description	Requirement	Part of this report
	External Scrutiny		
17AG(3)	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	Part 4
17AG(3)(a)	Information on judicial decisions decisions of administrative tribunals and by the Australian Information Commissioner that have had, or may have a significant effect on the operations of the entity.	If applicable, Mandatory	Part 4
17AG(3)(b)	Information on any reports on operations of the entity by the Auditor-General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, Mandatory	Part 4
17AG(3)(c)	Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	Not applicable
	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 4
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 G and 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 *Public Service Act 1999*.	Mandatory	Not applicable

PGPA Rule reference	Description	Requirement	Part of this report
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 F
17AG(4)(c)(iii)	A description of non-salary benefits provided to employees.	Mandatory	Part 4
17AG(4)(d)(i)	Information on the number of employees at each classification level who received performance pay.	If applicable, Mandatory	Not applicable
17AG(4)(d)(ii)	Information on aggregate amounts of performance pay at each classification level.	If applicable, Mandatory	Not applicable
17AG(4)(d)(iii)	Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, Mandatory	Not applicable
17AG(4)(d)(iv)	Information on aggregate amount of performance payments.	If applicable, Mandatory	Not applicable
	Assets Management		
17AG(5)	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, Mandatory	Part 4
	Purchasing		
17AG(6)	An assessment of entity performance against the *Commonwealth Procurement Rules*.	Mandatory	Part 4
	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 4
17AG(7)(b)	A statement that "*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]*".	Mandatory	Part 4
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 4

PGPA Rule reference	Description	Requirement	Part of this report
17AG(7)(d)	A statement that *"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."*	Mandatory	Part 4
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 4
17AG(7A)(b)	A statement that *"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."*	Mandatory	Part 4
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.	If applicable, Mandatory	Part 4
	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.	If applicable, Mandatory	Part 4

PGPA Rule reference	Description	Requirement	Part of this report
	Small business		
17AG(10)(a)	A statement that "*[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.*"	Mandatory	Part 4
17AG(10)(b)	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	Part 4
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*."	If applicable, Mandatory	Part 4
	Financial Statements		
17AD(e)	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	Part 5 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 E
17AD(f)	**Other Mandatory Information**		
17AH(1)(a)(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."*	If applicable, Mandatory	Part 4
17AH(1)(a)(ii)	If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, Mandatory	Not applicable
17AH(1)(b)	A statement that *"Information on grants awarded by [name of entity] during [reporting period] is available at [address of entity's website]."*	If applicable, Mandatory	Not applicable
17AH(1)(c)	Outline of mechanisms of disability reporting, including reference to website for further information.	Mandatory	Part 4 and Appendix S

PGPA Rule reference	Description	Requirement	Part of this report
17AH(1)(d)	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	If applicable, Mandatory	Not applicable (FOI exempt)
17AH(1)(e)	Correction of material errors in previous annual report.	If applicable, Mandatory	Appendix K
17AH(2)	Information required by other legislation.	Mandatory	Part 4 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 *ASIO Annual Report 2024–25* tabled in parliament, including to **Appendix Q**, **Appendix R**, **Appendix S**, **Appendix T** and **Appendix U**.

List of annual report requirements under the ASIO Act

ASIO is required under 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 applications for 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 applications for 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 *ASIO Annual Report 2024–25* 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

AFP – Australian Federal Police

AGSVA – Australian Government Security Vetting Agency

AIC – Australian Institute of Criminology

AM – Member of Order of Australia

AN – Ammonium Nitrate

ANAO – Australian National Audit Office

ANZAC – Australian and New Zealand Army Corps

ANSTO – Australian Nuclear Science and Technology Organisation

APS – Australian Public Service

APSC – Australian Public Service Commission

APS Net Zero – Australian Public Service Net Zero 2030 Policy

ASA – Adverse Security Assessment

ASIC – Aviation Security Identification Card

ASIO – Australian Security Intelligence Organisation

ASIO Act – Australian Security Intelligence Organisation Act 1979

ASIO Amendment Act – Australian Security Intelligence Organisation Amendment Act 2020

AUKUS – Australia-United Kingdom-United States partnership

B

C

CCD – Commonwealth Climate Disclosure

CIBC – Critical Infrastructure Background Check

CO_2-e – Carbon dioxide equivalent

CPR – Commonwealth Procurement Rules

D

DCB – Departmental Capital Budget

DRC – Depreciated Replacement Cost

E

EL – Executive Level

F

Flight Crew – Flight Crew Licence

FOI Act – *Freedom of Information Act 1982*

FRR – Public Governance, Performance and Accountability (Financial Reporting) Rule 2015

G

GST – Goods and Services Tax

H

HR – Human Resources

I

ICT – Information, Communication and Technology

IGIS – Inspector-General of Intelligence and Security

IMVE – Ideologically motivated violent extremism

Independent Reviewer – Independent Reviewer of Adverse Security Assessments

Independent Reviewer – Independent Reviewer of Security Clearance Decisions

INSLM – Independent National Security Legislation Monitor

J

K

L

LGBTQIA+ – Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, Asexual and other sex, gender and sexually diverse individuals

M

MSIC – Maritime Security Identification Card

N

NACC – National Anti-Corruption Commission

NAIDOC – National Aboriginal and Islander Day Observance Committee

NHSC – National Health Security Check

NIC – National Intelligence Community

NSSIC – Naval Shipbuilding and Sustainment Identity Card

NV – Negative Vetting

O

OIGIS – Office of the Inspector-General of Intelligence and Security

ONI – Office of National Intelligence

P

PBS – Portfolio Budget Statement

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

PGPA Rule – Public Governance, Performance and Accountability Rule 2014

PJCIS – Parliamentary Joint Committee on Intelligence and Security

PMV – Politically motivated violence

PV – Positive Vetting

Q

QOPT – Radiological material and equipment check

R

RMVE – Religiously motivated violent extremism

S

SCSA – Security Clearance Suitability Assessment

SES – Senior Executive Service

SME – Small and Medium Enterprises

T

TS-PA – Top Secret–Privileged Access

U

UK – United Kingdom

US – United States

V

W

X Y Z

Glossary

Five-Eyes – an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom and the United States.

adverse security assessments – mechanism by which ASIO recommends a prescribed administrative action that would be prejudicial to the interests of a person to be taken or not taken, such as the refusal of a visa or cancellation of a passport.

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 – activities relating to Australia that are carried on by or on behalf of, are directed or subsidised by or are undertaken in active collaboration with, a foreign power, being activities that:

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

Index

A

Aboriginal and Torres Strait Islander 15, 59, 61

academia/academic 34, 36

Administrative Review Tribunal 55

adverse security assessment/s (ASA) 32, 51, 95, 96, 128

advertising 63, 125

APS Net Zero 2030 Policy 66, 110, 128

ASIO Budget Statement 2024–25 13

ASIO Corporate Plan 2024–28 12, 13, 20, 22, 24, 28, 34, 38

ASIO Diversity and Inclusion Council 58

ASIO Diversity and Inclusion Strategy 2021–24 58

ASIO employees 15, 57

asset management 66, 123

attack/s 4, 11, 21, 36, 37

Attorney-General 13, 113

Audit and Risk Committee (ARC) 47, 48, 53, 64

AUKUS 4, 36

AusTender 64, 65, 124

Australian Federal Police (AFP) 31, 37, 128

Australian Government Security Vetting Agency (AGSVA) 39, 40

Australian National Audit Office (ANAO) 53, 65, 71, 124

Australian Public Service (APS) 57, 66, 110, 122, 123, 128

Australian Security Intelligence Organisation Act 1979 (ASIO Act) 11, 57, 62, 67, 99, 113, 127

Australian Security Intelligence Organisation Amendment Act 2020 (ASIO Amendment Act) 113

Australia's Disability Strategy 2021–2031 63

B

border integrity 11

budget 13, 23, 38, 42, 66, 75, 76, 77, 78, 84, 88, 89, 93, 94, 120

Burgess, Mike iii, 7, 12, 14, 19, 100

C

Capability and Investment Committee 47, 48

capital 42, 77, 84, 93, 128

cash flows 78, 81, 85, 89

changes in equity 73, 77, 89

clearance/s 6, 27, 33, 35, 38, 40, 51, 97

climate 67, 110

Comcare 108

Commonwealth Child Safe Framework 62

Commonwealth Climate Disclosure 67, 110

Commonwealth Procurement Rules (CPR) 64, 65, 123

Commonwealth Risk Management Maturity Model 47

communal violence 11

community interference 36

compliance 47, 48, 52, 53, 64, 67, 82, 108, 121

comprehensive income 73, 75, 77, 81, 89

conspiracy 5

consultancy/ies 26, 64, 65, 123, 124

contract/s 64, 65, 66, 80, 83, 122, 123, 124

corporate governance 47, 52, 121

correction 114, 126

Counter Foreign Interference Taskforce 5

counter-espionage and foreign interference 5, 12, 22, 23, 24, 25, 26, 27

counter-terrorism 5, 12, 21, 22, 23, 28, 29, 30, 31, 32, 37, 50

Criminal Code 49, 50

D

Defence 4, 11, 24, 26, 30, 39

defence capabilities 4

defence system/s 11

deficit 42, 75, 76, 77, 82, 89

Department of Finance 64, 66, 100, 101, 102, 125

Department of Home Affairs 32, 35, 95

Department of Finance 66, 125

Departmental Capital Budget (DCB) 42, 93

depreciation 82

determination 14, 39, 53, 57, 59, 63, 71, 99, 100, 104, 122, 126

Director-General iii, 1, 7, 11, 12, 14, 19, 32, 34, 35, 36, 47, 48, 52, 53, 56, 65, 67, 71, 79, 86, 97, 99, 100, 126, 127

disability 58, 63, 107, 125

Disability Action Plan 2022–24 58

disrupt 4, 11, 21, 22, 23, 24, 25, 26, 28, 32, 35, 36

diversity 15, 57, 58, 59, 60, 61, 63

diversity networks 58, 60, 61

E

emissions 66, 67, 110, 111

Environment Protection and Biodiversity Conservation Act 1999 67, 110

espionage 4, 5, 6, 11, 12, 20, 21, 22, 23, 24, 25, 26, 27, 36, 50, 130

Executive Committee 47, 48, 53, 86, 87, 99

executive remuneration 99, 125

exempt contracts 65, 124

expenses by outcomes 94

external scrutiny 49, 122

extremism 4, 21, 28, 35, 37

F

Federal and High Court 56

financial performance 42, 80, 120

financial position 76, 79, 81, 85, 89

financial statements 42, 53, 66, 71, 79, 88, 125

Five Eyes 5, 37, 59, 130

foreign intelligence service/s 5, 24, 27

foreign interference 4, 5, 11, 12, 20, 21, 22, 23, 24, 26, 50, 130

Foreign Investment Review Board 26

fraud/fraud control iii, 54, 121

funding 42, 73, 84

G

gender 59, 60, 104, 105, 122

Goods and Services Tax (GST) 65, 79, 123, 124

governance 13, 14, 19, 23, 38, 39, 47, 48, 52, 53, 59, 63, 71, 79, 93, 94, 99, 104, 110, 114, 121, 126, 128, 129

greenhouse gas 66, 67, 110, 111

H

I

ideologically motivated violent extremism (IMVE) 21, 28

ideologies 4

incident/s 30, 62, 108, 109, 121

Independent National Security Legislation Monitor (INSLM) 50, 67

Independent Reviewer of Adverse Security Assessments (IRASA) 51, 95, 96

Independent Reviewer of Security Clearance Decisions (IRSCD) 51, 97, 98

industry 34

influence 6, 7, 11, 12, 20, 23, 26, 30, 34, 36, 47, 48

Influence and Impact Committee 47, 48

insider threat/s 26, 35, 38

Inspector-General of Intelligence and Security (IGIS) 39, 50, 62, 67, 97, 129

intelligence 4, 5, 6, 7, 11, 12, 14, 15, 24, 25, 27, 28, 30, 31, 32, 36, 38, 39, 47, 48, 49, 50, 52, 62, 63, 67, 94, 95, 97, 99, 113, 127, 128, 129, 130

international production order 67, 95, 127

J

Joint Counter Terrorism Team 32

K

key management personnel 86

L

law enforcement 4, 5, 22, 30, 31, 32, 36, 37, 55

Leader of the Opposition 67

legal matters 55

LGBTQIA+/LGBTQ+ 15, 60

M

market research 63

Middle East 4, 31, 36

Minister for Finance 14, 39, 53, 104, 126

Minister for Home Affairs 67, 71, 127

Minister's Guidelines 52

minors 4, 5, 30, 37, 62

N

National Security Hotline (NSH) 7

National Security Legislation 49, 50

national terrorism threat level 4, 31, 35

non-consultancy 64, 65, 124

O

operational activities 22, 23, 24, 26, 28, 30

organisational structure 14, 120

other highly paid staff 57, 99, 102

oversight 12, 23, 38, 39, 47, 49, 52, 53, 58, 62, 66

P

Parliamentary Joint Committee on Intelligence and Security (PJCIS) 49, 64, 65, 67

partnerships 5, 23, 38, 40

people with disability 63, 107

personnel security 26, 33

politically motivated violence 4, 11, 32

Portfolio Budget Statement (PBS) 88, 120

Positive Vetting (PV) 32, 33, 39, 40, 41

prosecution/s 29, 55

psychosocial 108, 109

Public Governance, Performance and Accountability Act 2013 (PGPA Act) 13, 14, 19, 20, 39, 47, 53, 59, 63, 71, 79, 84, 93, 94, 104, 119, 126

Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) 99, 114, 119, 120, 121, 122, 123, 124, 125, 126, 129

Purchasing 64, 123

Q

questioning warrants 67, 113, 127

R

radicalisation 5, 30, 37

recruitment 58, 63

Religiously motivated violent extremists 4, 21, 29

resource statement 93

risk management 47, 52, 110

S

sabotage 11, 26, 27, 50

salary 57, 83, 103, 123

security 2, 4, 5, 6, 7, 11, 12, 13, 15, 19, 20, 22, 23, 24, 25, 26, 27, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 47, 48, 49, 50, 51, 52, 55, 56, 60, 62, 64, 65, 67, 71, 94, 95, 97, 99, 103, 126, 127, 130

Security and Compliance Committee 47, 48

Security Clearance Suitability Assessment (SCSA) 27

security clearance/clearances 6, 27, 38, 40, 51, 55, 97, 98

security environment 2, 4, 11, 15, 20, 28, 31, 35, 36

security intelligence 6, 11, 12, 13, 38, 52, 67, 94, 95, 99, 130

security leads 34

Security Outlook 2030 6, 35

Senate Estimates 49

Senate Legal and Constitutional Affairs Committee 49

Senior Executive Service (SES) employees 57, 103, 123

small and medium enterprises (SME) 125

small business 66, 125

special intelligence operation authorisations/ authorities 67, 127

stakeholder survey 22, 23

stakeholder/s 6, 7, 22, 23, 24, 25, 26, 28, 29, 34, 35, 36, 38, 39, 40, 56

surplus 42, 82

sustainability 40, 112

T

technical assistance requests 67, 127

technology 5, 15, 26, 33, 37, 40, 63

telecommunications data 67, 127

terrorism laws 50

terrorism threat level 4, 7, 31, 35

terrorist attack/s 4, 21, 36

terrorist/s 4, 5, 21, 30, 36, 37, 50

threat assessment/TA 6, 34, 35

threat/s 2, 4, 6, 7, 11, 12, 13, 15, 20, 23, 24, 26, 28, 30, 31, 32, 34, 35, 36, 38, 50, 62, 94, 130

Top Secret–Privileged Access (TS-PA) 6, 12, 20, 23, 38, 40

transparency 7, 36, 39, 47, 53

U

United Nations Convention on the Rights of Persons with Disabilities 63

V

vetting 6, 12, 14, 15, 20, 23, 38, 39, 40, 41, 63

visa 32, 55, 95, 130

W

warrants 67, 113, 127

wellbeing 5, 37, 108

work health and safety 63, 108

workforce 5, 6, 38, 40, 41, 57, 58, 59, 60, 61, 62, 63, 104, 105, 106, 107, 108

workplace agreement 57

Workplace Gender Equality Act 2012 59

X

Y

Z


ASIO
asio.gov.au