Australian Government

Australian Security Intelligence Organisation

CORPORATE PLAN

2024–28



75

1949–2024

ASIO

Remembering the past, securing the future

© Commonwealth of Australia 2024

All material presented in this publication is provided under a Creative Commons BY Attribution 3.0 Australia licence (https://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 (https://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 (https://pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Contact us

Phone

General inquiries 1800 020 648

Business inquiries 02 6234 1668

Media inquiries 02 6249 8381

Email

media@asio.gov.au

Post

GPO Box 2176, Canberra ACT 2601

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.

Director-General's introduction

I am pleased to present the ASIO Corporate Plan for 2024–25 to 2027–28, as required under section 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

Dramatic shifts in geopolitics, technologies and capabilities have transformed the security environment since Ben Chifley established ASIO 75 years ago. But our mission remains the same: we protect Australia and Australians from threats to their security.

Our Corporate Plan lays out how we will deliver that mission and how we will measure our performance.

Countering Espionage and Foreign Interference

Threats to our way of life represent Australia's principal security concern.

Based on what ASIO is identifying, investigating, assessing and disrupting, more Australians are being targeted for espionage and foreign interference than ever before.

Multiple nations are seeking to covertly understand and shape Australia's politics and decision-making, our alliances and partnerships, our defence capabilities, and our economic and policy priorities.

They are trying to recruit elected officials on all sides of politics and at all levels of government, public servants, business executives, academics and leaders in our communities.

They are trying to steal Australia's secrets, our citizens' data and our intellectual property.

They are trying to monitor, threaten and even harm members of diaspora communities.

In 2024–25, ASIO will continue our high-tempo investigative and operational activities to detect and defeat these threats. We will evolve our most sensitive capabilities and sharpen our responses.

Countering Terrorism

While threats to our way of life represent Australia's principal security concern, threats to life are an enduring priority and we maintain a robust counter-terrorism capability.

The national terrorism threat level is POSSIBLE because we assess there is a realistic possibility of a terrorist attack or attack planning here in the next 12 months.

The conflict in the Middle East is resonating in Australia and divisive rhetoric has heightened community tensions. We are not seeing Australians travelling to join the terrorists in the Middle East as we did for the ISIL caliphate, however, and while there have been some violent incidents associated with public protests, we have not seen acts of terrorism directly inspired by the conflict.


2024



The threat from nationalist and racist violent extremism persists, with local white nationalist groups primarily focused on recruitment and radicalisation.

In both extremist cohorts – religious and ideological – ASIO is primarily concerned about the threat from lone actors, individuals or small groups moving to violence with little or no warning, using readily available weapons.

Influence and Impact

The scale and sophistication of the threats facing Australia requires an equally scaled and sophisticated response.

ASIO will work with governments, agencies, industries and academia to harden the security environment and make Australia a more resistant, resilient and ultimately harder target.

Recognising that security is a shared responsibility, in 2024–25 we will prioritise supporting the strengthening of security culture – the security-related values, mindsets and behaviours that are normalised within a workplace.

Effective security should be 3-dimensional:

Vertical – built into the foundations of an enterprise, not simply added on at the end.

Horizontal – reaching across all parts of an organisation.

Temporal – regularly updated and communicated.

Image (left to right)

Mike Noyes	Deputy Director-General Intelligence Service Delivery
Mike Burgess	Director-General of Security
Gus Gilmore	Deputy Director-General Vetting Service Delivery
Hazel Bennett	Deputy Director-General Enterprise Service Delivery

TOP SECRET-Privileged Access

For individuals with access to particularly sensitive information and capabilities, security vetting provides an additional layer of protection and assurance.

Security cleared personnel – insiders – are attractive targets for those trying to steal Australia's secrets, manipulate our decision-making and disrupt our economy.

The TOP SECRET-Privileged Access (TS-PA) Vetting Authority was created to counter these threats.

Centralising Australia's highest-level vetting functions within ASIO leverages our security intelligence functions, holdings and capabilities to enable more persistent validation of an individual's suitability to hold a security clearance.

TS-PA reform facilitates a stronger and more effective partnership between ASIO and the agencies which sponsor security clearance holders.

In 2024–25 ASIO will continue to grow our capacity to conduct TS-PA vetting. We will deliver critical project elements providing greater assurance and increased mobility – allowing employees already cleared at the highest-level to move between agencies more easily.

Conclusion

ASIO's mission is enabled by our people, practices, partnerships and technology, as well as trust, governance, accountability and transparency.

While all of these things are vital, our most important asset – our most critical capability – is our people. Their ongoing dedication, innovation, agility and ingenuity is a golden thread that runs through the 75 years of ASIO's history.

The security challenges confronting Australia are significant but not insurmountable. In its 75th year, ASIO remains well placed to secure Australia and protect its people.



Mike Burgess
Director-General of Security

[redacted]

17.9.62.

GLAD TO HAVE YOUR ANSWER IN TIME
URGENTLY NEED YOUR HELP
PLEASE COLLECT CONTAINER
ON THE FIRST LANDING OF THE
McELHONE STAIRS ON THE WAY
FROM VICTORIA ST TO COOPER
WHARF RD, WOOLLOOMOOLOO.
(REPEAT – McELHONE STAIRS)

CONTRAINER IS INSIDE
OF BASE OR IRON POST
OF RAILINGS BEFORE THE
SECOND FLIGHT OF STAIRS
OPPOSITE BENCH – SEE
DRAWING.
WAITING FOR YOU
NEAREST SATURDAY

Secret ink letter from Skripov to Marshall

ASIO Corporate Plan 2024–28

PURPOSE

ASIO protects Australia and Australians from threats to their security.

SECURITY INTELLIGENCE EFFECTS AND OUTCOMES

COUNTER-ESPIONAGE AND FOREIGN INTERFERENCE

Protect Australia and Australians from espionage, foreign interference and sabotage through the detection of adverse security events at their earliest stage.



COUNTER-TERRORISM

Protect Australia and Australians from violent extremism by anticipating threats and responding to changes in the security environment.



CAPABILITIES

PEOPLE

ASIO's people are fundamental to our business, and our culture enables their success. We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership at all levels.



PRACTICES

ASIO acts with authority to stay ahead of our adversaries through disciplined business processes and tradecraft. Our practices enable intelligence-led and risk-based planning, operational decision-making, prioritisation, and ensure the effective and efficient use of resources. We adapt and lead in developing security practices, operating with integrity and in compliance with the law.



PARTNERSHIPS

Security is a shared responsibility and ASIO delivers its mission through strong partnerships. These relationships span government, including the National Intelligence Community, law enforcement, our state and territory partners, international counterparts, industry, academia and the Australian public. We contribute our capabilities and experience to enhance the collective response to government.



CONTEXT AND EXTERNAL DRIVERS

Security outlook



Geopolitical shifts



Technology advancement





INFLUENCE AND IMPACT

Leverage our capabilities and insights to help stakeholders better understand, identify and manage sophisticated security threats.

TOP SECRET-PRIVILEGED ACCESS VETTING

Deliver high assurance and transferable security clearances to Australia's highest-cleared workforce to enable the government to better manage and combat threats to its information, people and assets.

TECHNOLOGY

ASIO uses a human-led, data-driven, technology-enabled approach to understand and respond to threats. We embrace new technologies, leverage automation, and seize opportunities to innovate, including working with Australian industry partners. ASIO's Capability Program ensures we keep in step with rapidly changing technologies and practices to provide the security assurance Australians expect.

ASSURANCE

Trust, governance, accountability and transparency are fundamental for achieving mission effects and intelligence outcomes. Our risk, compliance and governance frameworks ensure we act within the letter and the spirit of the law. ASIO delivers on its mission using rigorous internal controls, embracing independent external oversight while ensuring ASIO is free from any influences or considerations not relevant to its functions.

Legislative and policy environment

Community expectations

Fiscal and labour market conditions



Book camera for surveillance

ASIO's operating context and external drivers

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

Evolving threat environment

The threats facing Australia are more serious and sophisticated than ever before.

We are seeing more Australians being targeted for espionage and foreign interference than ever before. Hostile foreign states and their intelligence services are aggressively seeking secrets about Australia's defence capabilities, government decision-making, political parties, foreign policy, critical infrastructure, space technologies, academic and think tank research, medical advances, key export industries and personal information.

Our adversaries are willing to commit to complex, multi-year efforts to acquire our cutting-edge technologies, using espionage in all its forms – cyber, human intelligence, technical collection, and exploiting public information. This extends to targeting the Australian defence industry to seek information on AUKUS, submarine technology, missile systems and many other sensitive topics.

Foreign intelligence services are targeting all levels of government, business and academia, intimidating members of diaspora communities and seeking to interfere in our democratic institutions. The threat is pervasive, multifaceted and, if left unchecked, cumulative impacts could do serious damage to our sovereignty, values and national interest.

This is apparent in the threat of sabotage, particularly in relation to critical infrastructure, which could be committed by violent extremists or foreign states. The most immediate, low cost and potentially high-impact vector for sabotage is cyber, which may be used by nation states to gain persistent undetected access to critical infrastructure to enable sabotage in the future.

Terrorism remains a threat. While Australia's terrorist threats have reduced in volume, they have increased in complexity. The threat from religious and ideologically motivated violent extremism persists and there is the realistic possibility of a terrorist attack or attack planning in the next 12 months.

Geopolitical shifts

We are faced with deeply challenging geostrategic circumstances, which will continue to be a significant driver of Australia's security environment.

Australia is part of the most dynamic region in the world, the Indo-Pacific. The region is home to some of the planet's fastest growing populations, fastest growing economies and fastest military build-ups. It is also home to intensifying major power competition. This competition, and any resulting challenges and changes to the international order, will produce a more uncertain security environment for Australia.

Australia's historic AUKUS partnership with the UK and the US, along with other allies and partners, will be critical to sustaining peace, stability and prosperity around the world.

Technology advancement

The threat environment continues to be shaped by rapid technological change, hyper-connectivity, massive data and artificial intelligence. Australia continues to be targeted by sophisticated foreign adversaries that are effectively unconstrained by resources, ethics or laws. Cyber is a low-cost and potentially high-impact vector for espionage, foreign interference and sabotage. Encryption continues to make threats more difficult to detect.

To ensure ASIO remains ahead of Australia's adversaries, ASIO continues to implement the government's 2021 $1.25 billion investment in our most sensitive capabilities. This includes adoption of technologies like automation and artificial intelligence which assist ASIO to work at scale, collating and triaging lawfully collected data in timeframes that would not otherwise be possible. Whilst these capabilities provide operational and enterprise advantage, humans remain responsible and accountable for all ASIO's decision-making. Through ASIO's Capability Program, ASIO is adopting a human-led, data-driven, technology-enabled approach to threat detection.

ASIO continues to drive a culture of innovation in its technology capability, focusing on the 3–5 year horizon, by utilising disruptive approaches to innovation, deliberate engagement with commercial and security risks, focusing on new and emerging technologies, and benchmarking our capabilities against world's best practice.

Legislative and policy environment

Threats to security are increasingly intersecting and emerging from new places and blurring the distinctions between ASIO's legislated responsibilities.

Trust, governance, accountability and transparency are fundamental for achieving mission effects and intelligence outcomes. The legal frameworks that govern ASIO's powers provide assurance to Ministers, the parliament and the public, that ASIO will use its powers with propriety, lawfully, and with due regard for the privacy of Australians. As threats evolve to reshape our security environment, our legal framework needs to be fit-for-purpose to ensure we can continue to protect Australians.

ASIO must always balance the protection of Australians with the protection of their rights. These are complementary, not competing priorities.

ASIO is subject to rigorous oversight provided by the Inspector-General of Intelligence and Security – who has powers equivalent to a Royal Commission – and the parliament. ASIO welcomes the establishment of the National Anti-Corruption Commission (NACC), which is an important development in enhancing integrity in the Commonwealth public sector. ASIO is committed to ensuring our activities are always proportionate to the threat we are confronting, using the least intrusive methods possible.

Community expectations

ASIO's role is to protect Australia and Australians from threats to their security – Australians do not expect us to just respond to new threats, they expect us to anticipate them. Our ability to deliver our mission requires us to maintain the confidence and trust of the Australian people, and this is why we operate in proportion to the threats Australia faces and in line with the standards and expectations of the Australian community. Transparency and trust remain a key element of ASIO's agenda; however, ASIO will continue to protect its people, capabilities and operations.

Our governance processes guide us in achieving our mission and meeting public expectations of probity, accountability and transparency. ASIO delivers on its mission using rigorous internal controls, embracing independent external oversight while ensuring ASIO is free from any influences or considerations not relevant to its functions.

Fiscal and labour market conditions

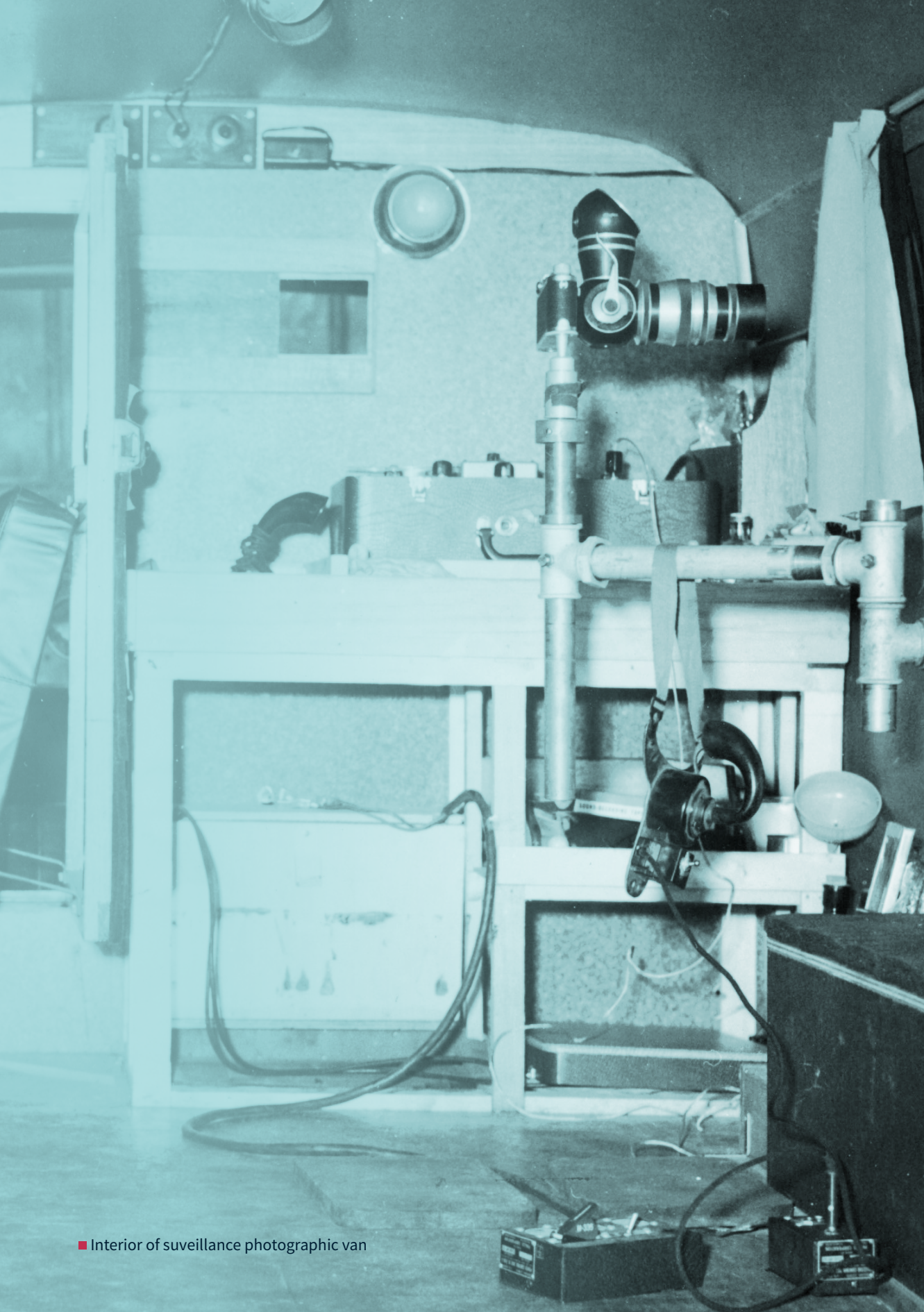
ASIO's most important capability is our people.

We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership at all levels.

ASIO recognises the importance of aligning our recruitment approach with Australia's employment and skills market. We continue to seek diverse skills for roles across our mission and enterprise, from intelligence analysts and technology specialists, to recruitment and finance officers.

Our people's agility and ingenuity, dedication and innovation allow us to keep pace with the threat environment and we are always on the lookout for creative thinkers who want to make a difference.

Australia faces long-term fiscal challenges due to climate change, an ageing population, regional security and rising demand for care and support services. ASIO operates responsibly to deliver its outcomes within the funding provided by government.



Interior of suveillance photographic van

Security intelligence effects and outcomes

ASIO will achieve its purpose for the 2024–28 period, through 4 key areas of focus delivering security intelligence effects and outcomes:

1. Counter-espionage and foreign interference
2. Counter-terrorism
3. Influence and impact
4. Top Secret-Privileged Access Vetting.

Two of these security intelligence effects and outcomes – counter-espionage and foreign interference, and counter-terrorism – are fundamental and enduring activities for ASIO.

Influence and impact continues to demonstrate the strategic importance we place on maximising the effect of our advice and insights so stakeholders can better understand, identify and manage sophisticated security threats.

The scale and sophistication of the threats facing Australia demands robust and resilient security settings. Vetting is a key component of this; only appropriately cleared people should have access to our nation's most sensitive secrets. The Top Secret-Privileged Access Vetting capability recognises the work ASIO is doing to progress the delivery of high assurance and transferable security clearances to Australia's highest-cleared workforce. This capability will enable the government to better manage and combat threats to its information, people and assets.

ASIO's performance against these 4 security intelligence effects and outcomes will be measured through a combination of quantitative and qualitative methods, including defined targets, case studies, stakeholder feedback, and identified milestones. ASIO will continue to progressively refine our performance measures to ensure we demonstrate our effectiveness in a transparent way, while safeguarding our sensitive capabilities and tradecraft.

Counter-espionage and foreign interference

Espionage and foreign interference together comprise ASIO's principal security concern. We will collect and analyse intelligence to uncover early, and resolve quickly, threats to Australian Government, defence, political and other national interests. Over the period of this Corporate Plan our advice will shape government decisions and inform tactical operations to protect Australia and Australians from espionage, foreign interference and sabotage. Our impactful and trusted advice to government, business, academia, industry and the public will raise awareness of the threat and establish a less permissive environment for covert actors. We will work with partners to disrupt and deter those attempting to undermine our national interests.

Counter-terrorism

ASIO will protect Australia and Australians from violent extremism by anticipating threats and responding to changes in the security environment. Australia remains a terrorist target. Some religiously motivated violent extremists aspire to undertake attacks here, but most currently have a limited intent to act. ASIO remains concerned about lone actors moving from talk to action without warning. The threat from nationalist and racist violent extremism also persists.

We have observed a shift in the range of political objectives with localised issues driving ideologies and beliefs. There has been an increase in violent rhetoric directed at or between groups in the Australian community in response to international events and domestic grievances. Some individuals have resorted to violence in response to perceptions their concerns are not being adequately addressed by authorities.

ASIO will prioritise our resources against the greatest threats, and will continue to collect intelligence within Australia and overseas, analyse and investigate terrorist threats, and work with partners to strengthen public safety and intervene to disrupt attacks. Our intelligence collection, investigation and assessment efforts enable ASIO to identify and understand the threats we face, and to provide impactful advice that hardens the environment against, and informs government policy and responses to, violent extremism.

Over the period of this Corporate Plan, we will continue to deliver impactful, relevant and practical advice to assist stakeholders in their counter-terrorism decision-making. Our advice will enable our stakeholders and partners to harden the environment and disrupt violent extremist activities.

Influence and impact

The scale and sophistication of the threats facing Australia requires ASIO to be proactive in its advice to government, business, academia, industry and the public. ASIO will leverage our capabilities and insights to help stakeholders strengthen their security culture and uplift their understanding and practices in relation to sophisticated security threats. Security culture encompasses all the characteristics, attitudes and habits of an organisation that establish and maintain the security of its people, information and assets. ASIO will publish a framework to help organisations build and maintain robust security practices and will continue to promote security awareness and strengthen security maturity by providing expert insights and impactful advice.

Top Secret-Privileged Access Vetting

In an environment where espionage and foreign interference is our principal security concern, ASIO will deliver Australia's highest-level security clearances for the Commonwealth to ensure government's most sensitive information, capability and secrets remain protected.

We will leverage ASIO's security intelligence functions, holdings and capabilities to allow a holistic assessment of a person's suitability to hold the highest-level security clearance, having regard to the most current and accurate information about the security threats confronting Australia.

Performance measures

Impact definitions* – the definitions to be shared with key stakeholders when determining what level of impact our advice has had on their decision-making.

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

Advice – for the purposes of this performance framework, 'advice' encompasses all forms of communication – to the Australian Government, government agencies, and industry and community sector stakeholders – that conveys ASIO's expertise, intelligence, assessments, priorities and recommendations on security matters.

**Impact definitions relate to counter–espionage and foreign interference and counter-terrorism measures.*

Counter-espionage and foreign interference

1. Impact of 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.			
Targets (% and impact level)	2024–25	2025–26	2026–27	2027–28
	90% MEDIUM – HIGH > 1 case study	90% MEDIUM – HIGH > 1 case study	90% MEDIUM – HIGH > 1 case study	90% MEDIUM – HIGH > 1 case study
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats. Case studies demonstrate the depth and breadth of ASIO operational activity in understanding, disrupting and hardening the environment from espionage and foreign interference, reducing harm to Australia and Australians.			
Methodology	Assessment of the impact of advice is drawn from examples of stakeholder feedback or case studies throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise ■ ongoing, frequent recipients of ASIO counter-espionage and foreign interference advice ■ engaged in counter-espionage and foreign interference operational activities, managing security risks, and/or disrupting espionage and foreign interference activities that threaten Australia's security. Assessment of the impact of operational activities is drawn from case studies which are provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's operational activities in disrupting and reducing the harm of espionage, foreign interference and sabotage. Case studies will be chosen early in the financial year on the basis of their potential to demonstrate the impact of operational activity, with consideration to protecting sensitive tradecraft, capabilities and information.			

Counter-terrorism

2. Impact of 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.			
Targets (% and impact level)	2024–25	2025–26	2026–27	2027–28
	90% MEDIUM – HIGH > 1 case study	90% MEDIUM – HIGH > 1 case study	90% MEDIUM – HIGH > 1 case study	90% MEDIUM – HIGH > 1 case study
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats. Case studies demonstrate the depth and breadth of ASIO operational activity in understanding, disrupting and hardening the environment from terrorism, reducing harm to Australia and Australians.			
Methodology	Assessment of the impact of advice is drawn from examples of stakeholder feedback or case studies throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise ■ ongoing, frequent recipients of ASIO counter-terrorism advice ■ engaged in counter-terrorism-related operational activities, managing security risks, and/or disrupting terrorism-related activities that threaten Australia's security. Assessment of the impact of operational activities is drawn from case studies which are provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's operational activities in disrupting and reducing the harm of violent extremism. Case studies will be chosen early in the financial year on the basis of their potential to demonstrate the impact of operational activity, with consideration to protecting sensitive tradecraft, capabilities and information.			

Influence and impact

3. 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.			
Targets	2024–25	2025–26	2026–27	2027–28
	> 1 case study	> 1 case study	> 1 case study	> 1 case study
Rationale	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 will leverage our capabilities and insights to help stakeholders better understand, identify and manage security threats. We will promote security awareness and strengthen security maturity by providing expert insights and impactful advice.			
Methodology	Assessment of the impact of Organisational activities and advice is drawn from case studies which are provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's activities and advice which contribute to protecting Australia and Australians from threats to their security. Case studies will be chosen early in the financial year on the basis of their potential to demonstrate the impact and influence of ASIO activities and advice, with consideration to protecting sensitive tradecraft, capabilities and information.			

Top Secret-Privileged Access Vetting

4. Top Secret-Privileged Access Vetting delivery

Measure	High assurance and transferable security clearances are issued to Australia's highest-cleared workforce.
Targets	As the Top Secret-Privileged Access Vetting function matures, ASIO will meet the agreed demand of security clearances in accordance with agreed targets and the agreed vetting standard to enable the government to better manage and combat threats to its information, people and assets. 2024–25: Programmatic oversight as ASIO builds capabilities to service future security clearance demand and continues to focus on delivering quality assurance. 2025–28: Quantitative measures will be introduced to complement qualitative measures of capability.
Rationale	ASIO will modernise and harden Australia's highest-level of security clearance in response to the unprecedented threat from espionage and foreign interference confronting Australia. In a phased approach commensurate with the resources made available to ASIO, we will mature productivity measures and targets; develop the necessary policy frameworks; and modernise enabling capabilities to provide government and other stakeholders high assurance and transferable security clearances.
Methodology	Qualitative and quantitative analysis of the capability will be 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 time frame. Consideration was given to including Key Performance Indicators (KPIs) in 2024–25 as a quantitative measure, however KPIs are not considered a useful measure to demonstrate progress in the current implementation phase of the Top Secret-Privileged Access Vetting function. KPIs will be progressively implemented from 2025–26 through 2027–28 to measure performance as ASIO transitions from a capability development focus to an operational model alongside ongoing capability targets.

Capabilities

ASIO's capabilities are our people, practices, partnerships, technology and assurance. ASIO continues to implement a range of strategies and plans to ensure we are continuing to evolve our capability in an effort to effectively and efficiently deliver on our purpose and undertake our key activities. The successful adoption of change associated with these strategies and plans will necessarily be underpinned by effective change management and consultation. ASIO is committed to applying the principles of the APS Strategic Commissioning Framework.

People



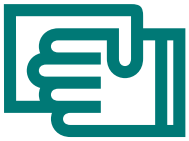
ASIO's people are fundamental to our business, and our culture enables their success. We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership and accountability at all levels. As part of our people strategy, we continue to implement our 5-year *Workforce Plan 2025* to ensure the Organisation is well positioned to meet current and future workforce challenges. ASIO strives to reflect the society we protect – we do not discriminate against individuals on the basis of gender, sexual orientation or cultural or ethnic origins.

Practices



ASIO acts with authority to stay ahead of our adversaries through disciplined business processes and effective operational and analytical tradecraft. Our practices enable rigorous analysis, assessment and advice, intelligence-led and risk-based planning, operational decision-making, prioritisation, and ensure the effective and efficient use of resources. We adapt and lead in developing security practices, operating with integrity, proportionality and in compliance with the law.

Partnerships



Security is a shared responsibility and ASIO delivers its mission through strong partnerships. These relationships span government, including the National Intelligence Community, law enforcement, our state and territory partners, international counterparts, industry, academia and the Australian public. Partnerships are critical and we contribute our capabilities and experience to enhance the collective response to government.

Technology



ASIO uses a human-led, data-driven, technology-enabled approach to understand and respond to threats. We embrace new technologies, leverage automation, and seize opportunities to innovate, including working with Australian industry partners. ASIO's Capability Program ensures we keep in step with rapidly changing technologies and practices to provide the security assurance Australians expect.

Assurance



Trust, governance, accountability and transparency are fundamental for achieving mission effects and intelligence outcomes. Our risk, compliance and governance frameworks ensure we act within the letter and the spirit of the law. ASIO delivers on its mission using rigorous internal controls, embracing independent external oversight while ensuring ASIO is free from any influences or considerations not relevant to its functions.

Risk management and oversight

The Director-General is responsible for ensuring ASIO maintains an appropriate system of risk oversight and management to ensure ASIO can fulfil its purpose. Accepting and engaging with risk is inherent to ASIO's role of protecting Australia and Australians from threats to their security.

ASIO manages its risks through our enterprise risk management framework and corporate governance committees. ASIO's enterprise risk management framework seeks to embed risk management into the culture and work practices of the organisation in order to maximise opportunities and manage uncertainty. ASIO engages with risk in all aspects of our business, and applies a sophisticated understanding of risk management practices to identify, evaluate and respond to risks and opportunities. ASIO maintains compliance with all elements of the Commonwealth Risk Management Policy, demonstrating our commitment to an appropriate system of risk oversight and management.

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.

The Executive Committee is supported in its consideration of ASIO's risk by the:

- Security and Compliance Committee, which 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, which 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, which makes recommendations to the Executive Committee on significant matters relating to or impacting on ASIO's influence agenda and gives account of performance against ASIO's objectives and endorsed lines of effort.

The Audit and Risk Committee provides independent assurance and advice to the Director-General, including on ASIO's enterprise risk management framework and internal controls for the effective oversight of risks.


Audit and Risk Committee
(Quarterly)
Chaired by external member
Independent advisory committee to the Director-General on the design, operation and performance of ASIO's internal governance, risk and control frameworks and compliance
Director–General of Security
Executive Committee
(Fortnightly)
Chaired by the Director-General of Security
Primary decision-making committee in ASIO
Security and Compliance Committee
(Monthly)
Chaired by Deputy Director-General Intelligence Service Delivery
Primary advisory committee to Executive Committee on organisational security and compliance matters
Influence and Impact Committee
(Monthly)
Chaired by Principal Advisor to the Director-General
Primary advisory committee to Executive Committee on influence and impact matters
Capability and Investment Committee
(Monthly)
Chaired by Deputy Director-General Enterprise Service Delivery
Primary advisory committee to Executive Committee on organisational capability and investment matters

Key risks

ASIO faces a broad range of risks reflecting its responsibilities as Australia's security intelligence organisation. The risks arising from ASIO's work can be significant but we are committed to engage with risk to protect Australia and Australians from threats to their security.



Legal and propriety

Risks to compliance with laws, regulations, direction from government, international obligations, internal procedures or standards of propriety.



Financial

Risks to the security of money, assets and resources, including our financial sustainability.



Capability

Risks to the effectiveness and robustness of ASIO's capabilities, including technologies, data, facilities, partnerships, people and operational capabilities.



Health and safety

Risks to the health, safety and wellbeing of staff, partners, affiliates and the public.



Security

Risks to the protection of ASIO's capabilities, information and activities from compromise.



Reputation

Risks to the preservation of trust and confidence that government and the public place in ASIO.





asio.gov.au