

Australian Government

Australian Security Intelligence Organisation

CORPORATE PLAN 2023–27

ASIO

Securing Australia—protecting its people

© Commonwealth of Australia 2023

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 April 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).

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

ASIO acknowledges the traditional owners and custodians of country throughout Australia and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, the cultures and elders past, present and emerging.

Director-General's introduction

I am pleased to present the ASIO Corporate Plan for 2023–24 to 2026–27, as required under section 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

The Corporate Plan lays out how we will achieve our purpose of protecting Australia and Australians from threats to their security, and how we will measure our performance.

ASIO's priorities for 2023–24 to 2026–27 reflect a complex, challenging and changing security environment—particularly the unprecedented level of threat from espionage and foreign interference.

In response, ASIO is leaning into the complexity, confronting the challenge and evolving to stay ahead of the change.

Operational outcomes

The scale and sophistication of the threats facing Australia requires a scaled and sophisticated response. When I commenced as Director-General, I prioritised operational outcomes. We must not just detect threats; we must defeat them.

I am proud of the operational work ASIO has done in response to this challenge. We have manifestly reduced harm. In the last twelve months alone, a significant number of foreign intelligence operatives and their proxies have either been removed from Australia or rendered inoperative.

In April, as a direct result of an ASIO investigation, the Australian Federal Police charged an Australian citizen with foreign interference offences.

From past experience, we expect the prosecution will have a 'chilling' effect on hostile foreign intelligence services—but it is critical to note that law enforcement action is only one weapon in the nation's arsenal.

In recent years, a substantial number of intelligence-led disruptions, visa cancellations and other actions have quickly, quietly and efficiently eliminated harm.

ASIO's capability

Operational success relies on being able to do things our adversaries believe are impossible.

We need to be able to 'collect the dots' from sophisticated foreign adversaries that are effectively unconstrained by resources, and use technology and encryption to hide their activities.

We need to be able to 'connect the dots' when the volume and complexity of data is expanding at exponential rates.



ASIO is utilising a human-led, data-driven, technology-enabled approach to future-proof our most sensitive capabilities.

ASIO's technical workforce is partnering with Australian industry to accelerate and sustain our ability to stay ahead of the threat.

Vetting uplift

On 1 July 2023, the *ASIO Amendment Act 2023* came into effect. The legislation uplifts and hardens Australia's highest-level of security clearances in response to the espionage and foreign interference threat.

Centralising Australia's highest-level vetting functions within ASIO leverages the organisation's security intelligence functions and holdings to best assess a person's suitability for a clearance.

A consistent approach to issuing, maintaining and revoking Australia's highest level of security clearances maximises the benefits of shared services and will allow cleared employees to move between agencies more easily.

Influence and impact

The threat environment demands that we proactively make our economy, institutions and political systems more difficult and resilient targets for those seeking to undermine them.

Because security is a shared responsibility, ASIO is taking outreach and engagement to a new strategic level. We are leveraging our capabilities and insights to help government, industry and academia better understand, identify and manage sophisticated security threats.

We are promoting security awareness—particularly of insider threats—and growing security maturity by providing expert insights and impactful advice.

Threat to life

While countering threats to our way of life is absorbing the majority of ASIO's resources, threats to life will always remain a priority.

Late last year, I lowered the national domestic terrorism threat level from PROBABLE to POSSIBLE.

This does not mean the threat is extinguished. Far from it. There remains a fifty per cent chance there will be an attempted terrorist attack in the next year—most likely by an individual or small group using a basic weapon—although, of course, ASIO will work around the clock to prevent it.

Even with a lower threat level, the counter-terrorism mission remains challenging and the operational tempo remains high.

Image (left to right)

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

Significant challenges and changes in the onshore security environment are adding to its complexity.

The reach of extremist content online means individuals are radicalising very quickly—in days and weeks—and I remain concerned by the number of young Australians being attracted to both ideologically and religiously motivated violent extremism.

Conclusion

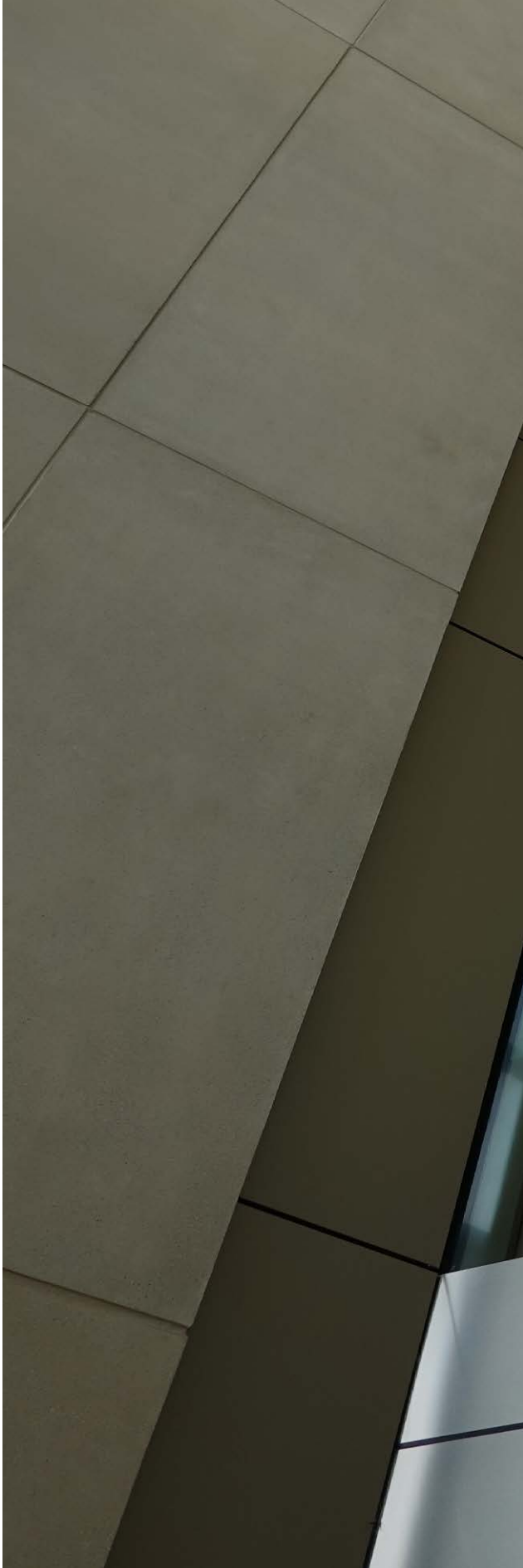
ASIO's mission is enabled by our people, practices, partnerships and technology, as well as the trust, governance, accountability and transparency that I take so seriously.

While all of these things are vital, I believe our most important asset—our most critical capability—is our people. They are ordinary Australians who do extraordinary things. Their agility and ingenuity, dedication and innovation will allow us to achieve the security effects and outcomes presented in this Corporate Plan.

The security challenges confronting Australia are significant, but ASIO remains well placed to secure Australia and protect its people.



Mike Burgess
Director-General of Security





ASIO Corporate Plan 2023–27

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





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.

Espionage and foreign interference has surpassed terrorism as ASIO's principal security concern. Foreign intelligence services are seeking to penetrate government, defence, academia and business to steal classified information, military capabilities, policy plans, and sensitive research and innovation. They are targeting all levels of government, intimidating members of diaspora communities and seeking to interfere in our democratic institutions. The threat is pervasive, multifaceted and, if left unchecked, could do serious damage to our sovereignty, values and national interest.

Australia's national terrorism threat level was lowered from PROBABLE to POSSIBLE in November 2022. ASIO assesses that Australia remains a potential terrorist target, but there are fewer extremists with the intention to conduct an attack onshore than there were when the threat was raised in 2014. However, despite the lower threat level, the counter-terrorism mission remains challenging and the operational tempo is not diminishing.

Geopolitical shifts

Geopolitical strategic shifts will continue to be a significant driver of Australia's security environment. Global power dynamics and the impacts of foreign conflicts, health and economic crises—as well as political polarisation and nationalism—will continue to shape and challenge Australia in complex ways.

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.

Broader Australian Government efforts to promote and build a resilient Indo-Pacific—including through our regional partnerships, our Quad relationships and the AUKUS trilateral security pact—will present a range of security opportunities and challenges.

In addition to these challenges, we can expect to see a complex and changing security environment as a result of climate change, global economic challenges and competition for resources over the next decade.

Technology advancement

The threat environment is increasingly volatile and shaped by a range of diverse drivers, including 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. Encryption continues to make threats to life from lone actors or small groups more difficult to detect.

To ensure ASIO remains ahead of Australia's adversaries, ASIO continues to implement the government's $1.25 billion investment in our most sensitive capabilities. Through ASIO's Capability Program, ASIO is adopting a human-led, data-driven, technology-enabled approach to threat detection.

ASIO's Office of the Future Technology Advisor continues to drive a culture of innovation in ASIO, 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 rapidly evolving technology and use of data continues to reshape our security environment, we need to ensure our legal framework remains fit-for-purpose to ensure we can continue to protect Australians as the technology environment changes.

ASIO must always balance the protection of Australians with the protection of their rights. These are not seen as competing priorities. To the contrary, they are complementary 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 is committed to ensuring our activities are always proportionate to the threat we are confronting, using the least intrusive methods possible and always acting within the letter and the spirit of the law.

Community expectations

ASIO's role is to protect Australia and Australians from threats to their security, therefore our ability to deliver our mission requires us to maintain the confidence and trust of the Australian people. 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 and 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, from technologists to psychologists, intelligence officers to corporate professionals.

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



Security intelligence effects and outcomes

ASIO will achieve its purpose for the 2023–27 period, through four key areas of focus delivering security intelligence effects and outcomes:

1. Counter-espionage and foreign interference;
2. Counter-terrorism;
3. Influence and impact; and
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 introduction of the Top Secret-Privileged Access Vetting security intelligence effects and outcomes 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 four 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 and industry 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. While Australia's national terrorism threat level is POSSIBLE, ASIO assesses that Australia remains a potential terrorist target. ASIO will prioritise our resources against the greatest threats, and the Organisation 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 and industry. ASIO will leverage our capabilities and insights to help stakeholders better understand, identify and manage sophisticated security threats. We will 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 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.			
Targets (% and impact level)	2023–24 90% MEDIUM - HIGH	2024–25 90% MEDIUM - HIGH	2025–26 90% MEDIUM - HIGH	2026–27 90% MEDIUM - HIGH
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.			
Methodology	Assessment of the impact is drawn from stakeholder feedback 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; and ■ 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.			

2. Impact of policy development 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 relation to specific and relevant espionage and foreign interference policy development and responses to this threat.			
Targets (% and impact level)	2023–24 90% MEDIUM - HIGH	2024–25 90% MEDIUM - HIGH	2025–26 90% MEDIUM - HIGH	2026–27 90% MEDIUM - HIGH
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.			
Methodology	Assessment of the impact is drawn from stakeholder feedback 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; and ■ engaged in developing relevant policy responses to the espionage and foreign interference threat.			

Counter-terrorism

3. Impact of operational activities 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.			
Targets (% and impact level)	2023–24 90% MEDIUM - HIGH	2024–25 90% MEDIUM - HIGH	2025–26 90% MEDIUM - HIGH	2026–27 90% MEDIUM - HIGH
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.			
Methodology	Assessment of the impact is drawn from stakeholder feedback 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; and ■ engaged in counter-terrorism-related operational activities, managing security risks, and/or disrupting terrorism-related activities that threaten Australia's security.			

4. Impact of policy development 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 specific and relevant policy development and responses to terrorism.			
Targets (% and impact level)	2023–24 90% MEDIUM - HIGH	2024–25 90% MEDIUM - HIGH	2025–26 90% MEDIUM - HIGH	2026–27 90% MEDIUM - HIGH
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.			
Methodology	Assessment of the impact is drawn from stakeholder feedback 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; and ■ engaged in developing relevant policy responses to terrorism.			

Influence and impact

5. Delivery of impactful intelligence and advice

Measure	Case studies which demonstrate the delivery of impactful intelligence and advice, resulting in an operational outcome or policy reform.			
Targets	2023–24	2024–25	2025–26	2026–27
	≥ 1	≥ 1	≥ 1	≥ 1
Rationale	The scale and sophistication of the threats facing Australia require ASIO to be proactive in its advice to government and industry. 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	Case studies are provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's intelligence and advice for our stakeholders. Case studies will be chosen at the beginning of the financial year on the basis of their demonstration of the impact of ASIO assessments and advice with consideration to protecting sensitive tradecraft, capabilities and information.			

Top Secret-Privileged Access Vetting

6. Top Secret-Privileged Access Vetting delivery

Measure	High assurance and transferable security clearances are issued to Australia's highest cleared workforce.
Targets	2023–27 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.
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.

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.

People



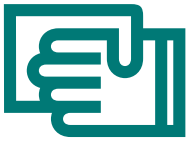
ASIO's people are fundamental to our business, and our culture enables their success. We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership and accountability at all levels. As part of our people strategy, we continue to implement our five-year *Workforce Plan 2025* to ensure the Organisation is well positioned to meet current and future workforce challenges. ASIO's *Diversity and Inclusion Strategy 2021–24* is ASIO's roadmap for prioritising action and monitoring the progress of our diversity and inclusion objectives.

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. 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; and
- 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.



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