Australian Government

Australian Security Intelligence Organisation

Corporate Plan

2017–18

www.asio.gov.au

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://www.itsanhonour.gov.au/coat-arms/index.cfm).

Contact us

Phone

General inquiries 02 6249 6299 or 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

Contents

Director-General's introduction 1

ASIO's purpose 2

Security and operating environment 5

Performance 7

Capability 8

Risk oversight and management 9

Director-General's introduction

I am pleased to present the 2017–18 Australian Security Intelligence Organisation (ASIO) corporate plan, which covers the period of 2017–18 to 2020–21, as required under paragraph 35(1)(b) of the Public Governance, Performance and Accountability Act 2013.

This plan comes at a time when Australia is facing significant security challenges. Threats from terrorism, espionage and foreign interference are unprecedented and will remain at heightened levels for years to come. The environment in which ASIO and our national security partners are working to protect the nation and its people is more complex and dangerous.

These features of the security and operating environment will continue to stretch our people, resources and capabilities. We will not be able to comprehensively mitigate all security risks. We will need to continue to prioritise our efforts, focusing on the sources of greatest potential harm and the areas where our advice and operational activities can have the greatest impact.

Against this background, this plan establishes the framework that we will use to measure and assess our performance against our four strategic priorities for the period of 2017–18 to 2020–21:

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

I am committed to ensuring that ASIO performs effectively and meets the expectations of the Australian Government, government agencies and industry stakeholders. In the current security and fiscal environments, it is more important than ever that we are 'hitting the mark'. To that end, I have instituted an annual survey of our senior stakeholders to hear directly from them how well ASIO is meeting their needs and how we can better support them. I have also implemented a performance reporting regime for our internal governance committees to ensure we are well positioned to identify and address performance issues on a continuing basis.

While the challenges ahead are considerable, I am confident that ASIO, working closely with our national and international security partners, will continue to make a significant contribution to the security of Australia and its people.

Duncan Lewis AO DSC CSC
Director-General of Security

ASIO's purpose

ASIO is Australia's national security intelligence service. Our purpose is to protect Australia, its people and its interests from threats to security through intelligence collection and assessment, and the provision of advice to the Australian Government, government agencies and industry.

Our work is anticipatory. We seek to identify, investigate and assess potential security threats and to work with national and international security partners to prevent harm from occurring.

We harness our expertise in security, unique intelligence collection capabilities, strong national and international partnerships, and all-source intelligence analysis capabilities to provide trusted, actionable advice for our stakeholders.

A commitment to legality and propriety

In working to meet our purpose, we must operate in a manner that is consistent with our values of excellence, integrity, respect, cooperation and accountability.

These five values incorporate our firm commitment to operate lawfully, in proportion to threats we are investigating and in line with the standards and expectations of the Australian community. This commitment is deeply ingrained in ASIO's 'DNA'. A comprehensive oversight and accountability framework, comprising legislation and ministerial, parliamentary and independent oversight provides assurance that we will continue to meet our commitment.

Our values

Our values represent the day-to-day expectations of each person working in ASIO. You will see our commitment to these five values when we:

EXCELLENCE	INTEGRITY	RESPECT	COOPERATION	ACCOUNTABILITY
produce high-quality, relevant and timely advice, based on the best available information	are ethical and work without bias and within the law	show respect in our dealings with others	build a common sense of purpose and mutual support	are responsible for what we do and for our outcomes
display strong leadership and professionalism	maintain confidentiality and the security of our work		communicate appropriately in all our relationships	are accountable to the Australian community through the government and the parliament
improve through innovation and learning			foster and maintain productive partnerships	

ASIO exists to protect Australia, its people and its interests from threats to security

What we do

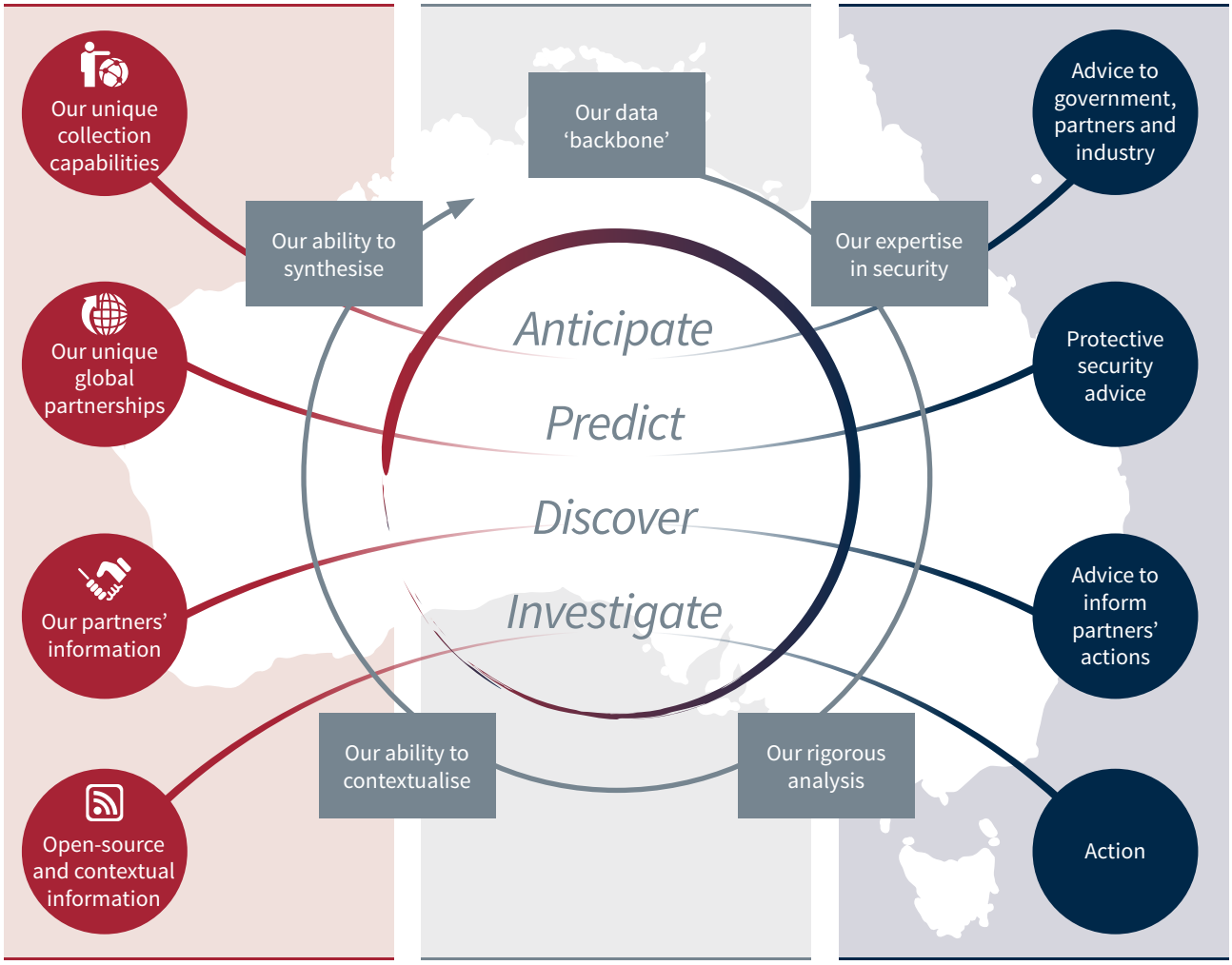
- Counter terrorism
- Counter espionage, foreign interference and malicious insiders
- Counter serious threats to Australia's border integrity
- Provide protective security advice to government and industry

How we do it

1 Harness our unique intelligence capabilities, partnerships and partner information

2 Apply rigorous data-driven analysis contextualised with our deep subject matter expertise

3 Anticipate threats and produce trusted and actionable advice to protect Australia




LOADING 100%
SEARCH
WORLD

Security and operating environment

ASIO's work throughout the period of this plan will be set against a steadily worsening security and operational environment.

Terrorism remains a serious security issue both globally and within Australia. Since the national terrorism threat level was raised to PROBABLE in September 2014, there have been five onshore terrorist attacks and 13 disruption operations in response to attack planning in Australia. The conflict in Syria and Iraq has shaped a generation of extremists in Australia who will present a security threat for at least the coming decade. Foreign fighters returning, or forcibly dispersed, from Syria and Iraq will also present a longer-term threat to Australians and Australian interests at home, in our immediate region and further abroad. ASIO's counter-terrorism investigative caseload has grown significantly in recent years, with a greater proportion of cases now involving higher levels of threat. Staying ahead of these threats will continue to put pressure on our resources and capabilities.

Terrorist attacks on law enforcement, military and security personnel in Australian and overseas demonstrate a very real threat to staff working to provide security for their nation and its people. Stronger protective and operational security measures will be required to allow our staff to operate safely and effectively in this environment.

Espionage and foreign interference directed against Australia, including by cyber means, will continue to occur on an unprecedented scale. These activities have the potential to cause serious harm to the nation's sovereignty, the integrity of our political system, our national security capabilities, our economy and other interests. Foreign investments in sensitive and critical national infrastructure that raise national security concerns will remain an important focus for us.

Rapidly changing technology and the widespread use of encryption are providing individuals and groups who are engaged in activities of security concern with tools to obscure their activities from security and law enforcement agencies. Along with our national and international partners, we will remain under pressure to develop and maintain technological and other capabilities that provide access to the information required to identify and disrupt harmful activities.

In this environment of heightened security threats, government and industry stakeholders are seeking more advice and closer engagement with ASIO to assist them to effectively manage security risks. Working in partnership with our stakeholders—providing advice, assessments and services—will be a priority for us over the period of this plan. This will, however, need to be balanced against the requirement to conduct the fundamental intelligence collection, investigation and assessment work that provides the basis for our advice to stakeholders. Maintaining this balance will be an ongoing challenge.

Additionally, the scale, complexity and interconnectedness of national security issues facing Australia is demanding greater collaboration and integration of effort among Australian and international security agencies. We will continue to work closely with our partner agencies to integrate our efforts, including by supporting the establishment of the Australian Government's new Home Affairs portfolio and implementation of the 2017 Independent Intelligence Review recommendations.

2017–18 PERFORMANCE FRAMEWORK

ASIO'S PURPOSE

To protect Australia, its people and its interests from threats to security through intelligence collection and assessment, and the provision of advice* to the Australian Government, government agencies and industry.

KEY ACTIVITIES

PERFORMANCE MEASURES

	1 Counter terrorism	2 Counter espionage, foreign interference and malicious insiders	3 Counter serious threats to Australia's border integrity	4 Provide protective security advice to government and industry
a	Our advice influences the Australian Government's policy development and responses to terrorism.	Our advice influences the Australian Government's policy development and responses to espionage, foreign interference and malicious insiders.	Our advice influences the Australian Government's policy development and responses to serious threats to Australia's border integrity.	Our protective security advice and services assist national security partner agencies to manage security risks.
b	National security partner agencies use our advice to disrupt and defend against terrorism.	National security partner agencies use our advice to disrupt and defend against harmful espionage, foreign interference and malicious insiders.	National security partner agencies use our advice to disrupt and defend against serious threats to Australia's border integrity.	Our engagement with at-risk industry sectors assists them to manage national security risks effectively.
c		We collect foreign intelligence in Australia that advances Australia's national security interests.		

INTENDED RESULTS

Our advice assists the Australian Government, national security partner agencies and industry to manage security risks and disrupt activities that threaten Australia's security.

TARGET FOR ACTIVITIES

Our stakeholders in the Australian Government, national security partner agencies and industry are satisfied with our advice and see ASIO as an effective national security partner.

*For the purposes of this performance framework, 'advice' encompasses all forms of communication to the Australian Government, government agencies and industry stakeholders that conveys ASIO's expertise, assessments and recommendations on security matters.

Performance

ASIO's performance framework is directly connected to our purpose: to protect the nation and its interests from threats to security through intelligence collection and assessment, and the provision of advice to the Australian Government, government agencies and industry.

For the period 2017–18 to 2020–21, we will pursue this purpose by focusing on four strategic priorities:

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

Our 2017–18 performance framework provides the measures for assessing our achievements. These measures will apply for each reporting period covered by this plan.

We will measure our performance by conducting an annual survey of our senior stakeholders in Australian Government, national security partner agencies and industry and seeking regular feedback from working-level stakeholders. Our performance assessments will also be informed by independent Australian Government evaluations of ASIO's intelligence performance.

ASIO's Intelligence Committee will monitor our performance against these measures throughout the year and report to ASIO's Executive Board, chaired by the Director-General. At the end of each financial year, we will provide an overall assessment of our performance in our annual performance statements. An unclassified version of these statements will be included in our annual report.

Capability

ASIO requires a wide range of capabilities to achieve our purpose. These include human and technical intelligence collection, surveillance, investigative, assessment and advice capabilities, all supported by effective corporate and enabling resources. Throughout the period of this plan, we will implement a range of strategies to build and sustain these capabilities.

Intelligence capability

We will continue to implement our counter-terrorism and counter-espionage and interference strategic plans, which are focused on building the capability of our staff to operate effectively in the security environment, reforming business practices to ensure we are making the most efficient use of resources, and integrating our efforts with partners to deliver the best possible security outcomes for Australia.

Under our technical capabilities strategy we are working to develop high-impact capabilities, embed technical knowledge and expertise in our workforce, collaborate with domestic and international partners on technical development, and maximise the efficiency and effectiveness of our investments and infrastructure.

Enterprise technology

Our enterprise technology strategy sets out how we will transform our information systems and business practices to improve our collection, management and exploitation of data. Under the strategy we will pursue enterprise technology that is seamlessly connected, agile, sustainable, accountable and enables a data-driven approach to our work.

Workforce capability

The ASIO capability framework provides the basis for achieving the 'people capability' we need. It establishes the core capabilities required by ASIO officers at all levels of the Organisation and provides pathways to meet learning and development needs. As part of the ASIO2020 program, we will pursue strategies to improve our career management arrangements and to strengthen workforce diversity and inclusion.

ASIO2020

ASIO2020 is our strategic organisational reform program. This program supports the development and implementation of reforms in four key areas—people, systems, culture and context. The broad objectives for these reforms are that:

People—our workforce is valued for its expertise, courage and diversity of background and experience. We use a best-practice career management framework to attract, develop, position and retain talent to deliver organisational needs;

Systems—our systems and use of technology are adaptive and formed through collaboration with partners, and grant ready access to data and information to produce timely and relevant intelligence;

Culture—we take pride in our past while looking to the future. We are an organisation that values the exploration of ideas and listens to, cares for, trusts and empowers its people as they work together to achieve a common mission; and

Context—we operate in an environment where our capabilities, advice and collaboration are sought after by partners, and where our contribution to national security is recognised and valued.

Risk oversight and management

Engaging with risk is central to ASIO's purpose and activities. We operate in an increasingly complex security environment, and risk management is critical to the security of our business and people.

Our approach to risk is informed by the ASIO Risk Management Policy, which sets out our risk appetite and philosophy. Our governance structure provides the framework for whole-of-organisation review and decision-making on risk management.

ASIO's Executive Board is the primary advisory committee that supports the Director-General in the governance of the Organisation. The board oversees our risk management policies, including the identification and treatment of strategic risks. It determines whether the overall level of risk we are carrying is acceptable and considers whether risk management structures, systems and processes remain effective.

ASIO's standing governance committees report to the Executive Board on our management of risks. In 2017–18, these committees will report risks in the following six categories:

- intelligence;
- capability;
- security;
- workforce;
- finance; and
- diversity and inclusion.

These governance committees will identify risk trends and developments, review risk levels, consider management strategies, determine action and escalate matters to the Executive Board for direction and decision-making as required.

The Audit and Risk Committee

The Director-General established the Audit and Risk Committee (ARC) in compliance with section 45 of the *Public Governance, Performance and Accountability Act 2013*. The ARC's role is to provide independent assurance and advice to the Director-General on the design, operation and performance of our internal governance, risk and control framework. The ARC has four external members including a chair. It reviews the effectiveness of our risk management framework and associated procedures for the identification and management of business and financial risks, including fraud.