Australian Government
Australian Security Intelligence Organisation

Corporate Plan

2016–17 to 2019–20



www.asio.gov.au

© Commonwealth of Australia 2016

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

Contact us

We welcome feedback on our corporate plan from any of our readers. Please contact:

Officer First Assistant Director-General, Executive

Phone *General enquiries* (02) 6249 6299 or 1800 020 648

Business enquiries (02) 6234 1668

Media enquiries (02) 6249 8381

Email media@asio.gov.au

Post GPO Box 2176, Canberra ACT 2601

Director-General's introduction



I am pleased to present ASIO's Corporate Plan 2016–17 for 2016–17 to 2019–20, as required under paragraph 35(1)(b) of the Public Governance, Performance and Accountability Act 2013.

This corporate plan is endorsed by our leadership team and describes how we will serve Australia and deliver public value by protecting the nation and its interests from threats to security through intelligence collection, assessment, and advice to government.

Over the life of this plan we will continue to partner with Australian and international intelligence, law enforcement and security agencies, and rely on the support of Australian people from all communities, to engage in five broad areas of security concern:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity;
- providing protective security advice to government and business; and
- collecting foreign intelligence in Australia.

We anticipate a series of challenges to these activities through the expanding variety of threat actors, threats developing more rapidly, society's use of online technologies, and the need to evolve key intelligence capabilities to match.

We are committed to meeting these challenges through the diversity and innovation of our people and through strategic capability development, in particular recruiting and retaining the best people and developing approaches to manage the increasing variety, velocity, and volume of data.

Expectations of ASIO from Australian governments, communities, and citizens have never been greater and we must strive to continue to deliver on their trust. The overall approach to performance measurement in this plan is to consider the effects generated in the management of risk by Australian governments and agencies as a result of our security advice, reporting, and services.

ASIO's leaders see in this corporate plan an agenda for the next four years that enables us to make a greater contribution than ever to protect Australia's prosperity. We will achieve this through effective partnering, development of vital intelligence capacities, and enabling preventative action to mitigate the very real security threats Australia faces. I commend the plan to you.

Duncan Lewis AO DSC CSC
Director-General of Security



Duncan Lewis
DIRECTOR-GENERAL OF SECURITY

Kerri Hartland
DEPUTY DIRECTOR-GENERAL

Tony Sheehan
DEPUTY DIRECTOR-GENERAL

Heather Cook
DEPUTY DIRECTOR-GENERAL

We want ASIO to be trusted and respected as a protector of Australia's national security, accessible to stakeholders, effectively communicating security risks, and an adaptive and innovative organisation whose prime asset is a diverse team of passionate people committed to serve the nation.

We are committed to ASIO's values of excellence, integrity, respect, cooperation and accountability and making a difference to achieving the organisation's purpose.

OUR VISION

ASIO's vision is to be trusted and respected as a protector of Australia's national security, to be accessible to partners, to effectively communicate security risks, to be an adaptive and innovative organisation and to have a diverse team of passionate people committed to serve the nation. This vision will drive us forward to achieving our purpose of protecting the nation from security threats.

OUR VALUES

Our values represent the day-to-day expectations on each person in ASIO in performing our vital work. You will see these values in action when we...

- **EXCELLENCE**
  - Produce high quality, relevant, timely advice based on the best available information
  - Display strong leadership and professionalism
  - Improve through innovation and learning
- **INTEGRITY**
  - Are ethical and work without bias within the law
  - Maintain confidentiality and the security of our work
- **RESPECT**
  - Show respect in our dealings with others
- **COOPERATION**
  - Build a common sense of purpose and mutual support
  - Communicate appropriately in all our relationships
  - Foster and maintain productive partnerships
- **ACCOUNTABILITY**
  - Are responsible for what we do and for our outcomes
  - Are accountable to the Australian community through the Government and the Parliament

About this Plan

This corporate plan is a key element of ASIO's strategic management and will support planning, performance, capability development, and risk activities across the organisation. The plan informs business planning and capability development by our work groups and teams, and will flow through to individual performance management discussions and planning with our people.

Our corporate plan contains some national security classified information. This detail will be removed from the version of the corporate plan made available publicly so as to avoid prejudice to a designated activity of ASIO, in accordance with determinations made by the Attorney-General and the Finance Minister under section 105D of the *Public Governance, Performance and Accountability Act 2013*.

ASIO's classified corporate plan is provided to the Attorney-General, the Finance Minister, the Parliamentary Joint Committee on Intelligence and Security, the Inspector-General of Intelligence and Security, and the Auditor-General. This plan is one way we can inform ministers and Parliament about our activities. The classified corporate plan is also shared with government stakeholders, including police, law enforcement and national security agencies.

Our unclassified corporate plan is available on our website – **www.asio.gov.au** – and is provided to business, the community, and the media.

ASIO's Purpose[1]

We have a single enduring purpose that delivers value for the public:

To protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for Government, government agencies, and business.

We work as part of a networked system of relationships across Australian society and internationally to achieve our purpose. Our approach is to directly engage with partners, to consider the impact of our advice, and to deliver actionable intelligence products and services, including so our partners can achieve their outcomes. Key to this is assistance provided by individual Australians, without whom we could not achieve our work.

To achieve our purpose, we adopt a risk-led approach in pursuing activities in five broad areas of security concern:

- countering terrorism and the promotion of communal violence
- countering espionage, foreign interference and malicious insiders
- countering serious threats to Australia's border integrity
- providing protective security advice to government and business
- collecting foreign intelligence in Australia.

Our work directly supports Australia's national security through contributing to:

- a safe and resilient population
- protecting and strengthening national sovereignty
- securing our national assets, intellectual property, infrastructure and institutions
- a favourable international security environment.

We expect our purpose and activities to endure. We will continue to:

- pursue intelligence that enables us to anticipate events and reduce the potential for harm to occur to the community and our national interest
- to communicate intelligence that enables other agencies to act and prevent security threats being realised
- inform government decision-making and policy settings to protect the public.

[1] ASIO's purpose directly maps to the single outcome in the Attorney-General's Portfolio Budget Statements 2016–17, available from www.ag.gov.au/Publications/Budgets.

About ASIO



ASIO was established in 1949 as Australia's national security intelligence service in a letter signed by then Prime Minister Ben Chifley. The Organisation was provided with a legislative framework in 1956 which has evolved[2] into the current *Australian Security Intelligence Organisation Act 1979* (the ASIO Act)[3]. The ASIO Act defines our roles and responsibilities, and is the legislative basis for our purpose, activities, and cooperation with partners.

Security and intelligence agencies perform an important function in modern societies. The Australian Government uses intelligence to pursue and protect our national interests and to inform its decision-making. Security intelligence is vital to protecting the nation and its people. Our role as the national security intelligence service is anticipatory and protective in nature: we are expected to detect and stop terrorist attacks and to thwart spies.

We have a staff of around 1,750 working across Australia's capital cities and a network of liaison offices overseas. This network supports relationships with more than 300 agencies in more than 120 countries. Our budget estimate is $445.2m for 2016–17.

Our resources will be deployed across hundreds of investigations and thousands of leads. We will collect intelligence through human intelligence, warranted activities and requests for protected data. We will deliver hundreds of thousands of security assessments and communicate thousands of intelligence products and pieces of advice to enable action to be taken.

We have three groups in our organisational structure:

- strategy
- counter-espionage and interference & capabilities
- and counter-terrorism.

This functional arrangement reflects the resources and governance required for our dominant and high-risk activities:

- countering terrorism and the promotion of communal violence
- countering espionage, foreign interference, and malicious insiders.

The structure is shown on pages 8–9.

[2] Two Royal Commissions by Justice Robert Marsden Hope AC CMC QC have shaped this evolution: the Royal Commission into Intelligence and Security 1974–1977 and the Royal Commission into Australia's Security and Intelligence Agencies 1984.

[3] The ASIO Act is available online from legislation.gov.au. The link to the compilation current at the time of writing this plan is www.legislation.gov.au/Details/C2016C00314

Organisation structure



Duncan Lewis
DIRECTOR-GENERAL OF SECURITY

DEPUTY DIRECTOR-GENERAL STRATEGY GROUP

First Assistant Director-General

- STATE MANAGER NSW NORTH
- EXECUTIVE
- STATE MANAGER VIC SOUTH
- CORPORATE & SECURITY
- OFFICE OF LEGAL COUNSEL
- TECHNICAL CAPABILITIES

Assistant Director-General

- OFFICE OF THE SENIOR EXECUTIVE
- STRATEGIC PARTNERSHIPS AND PRODUCTION
- ASIO2020
- STATE MANAGER QLD
- STATE MANAGER SA
- STATE MANAGER WA
- STATE MANAGER TAS
- TERRITORY MANAGER NT
- TERRITORY MANAGER ACT
- INTERNAL SECURITY
- FINANCIAL MANAGEMENT
- HUMAN RESOURCES
- PROPERTY
- SECURITY ASSESSMENTS, EMPLOYMENT & COMMERCIAL LAW
- LEGISLATION, WARRANTS & TECHNICAL CAPABILITIES
- LITIGATION
- OPERATIONS & CAPABILITY PROTECTION
- DATA & TECHNICAL ANALYSIS
- TELECOMMUNICATION OPERATIONS
- COMPUTER OPERATIONS
- CLOSE ACCESS OPERATIONS
- STRATEGY AND PERFORMANCE

[redacted]

DEPUTY DIRECTOR-GENERAL CEI & CAPABILITIES GROUP

- OPERATIONAL CAPABILITIES & TRAINING
  - PHYSICAL SURVEILLANCE
  - OPERATIONS SERVICES
  - TRAINING
- INFORMATION
  - IT INFRASTRUCTURE SERVICES
  - BUSINESS INFORMATION SYSTEMS
  - INFORMATION SERVICES
- COUNTER-ESPIONAGE & INTERFERENCE
  - COUNTER-ESPIONAGE & INTERFERENCE A
  - COUNTER-ESPIONAGE & INTERFERENCE B
  - COUNTER-ESPIONAGE & INTERFERENCE C
  - CYBER ESPIONAGE

DEPUTY DIRECTOR-GENERAL CT GROUP

- COUNTER-TERRORISM
  - COUNTER-TERRORISM COORDINATION
  - COUNTER-TERRORISM INVESTIGATIONS 1
  - COUNTER-TERRORISM INVESTIGATIONS 2
- SECURITY ADVICE & ASSESSMENTS
  - NATIONAL THREAT ASSESSMENT CENTRE
  - BORDER INVESTIGATIONS & ASSESSMENTS
  - INTELLIGENCE DISCOVERY, INVESTIGATIONS & ASSESSMENTS
- AUSTRALIAN COUNTER-TERRORISM CENTRE
  - AUSTRALIAN COUNTER-TERRORISM CENTRE



Environment

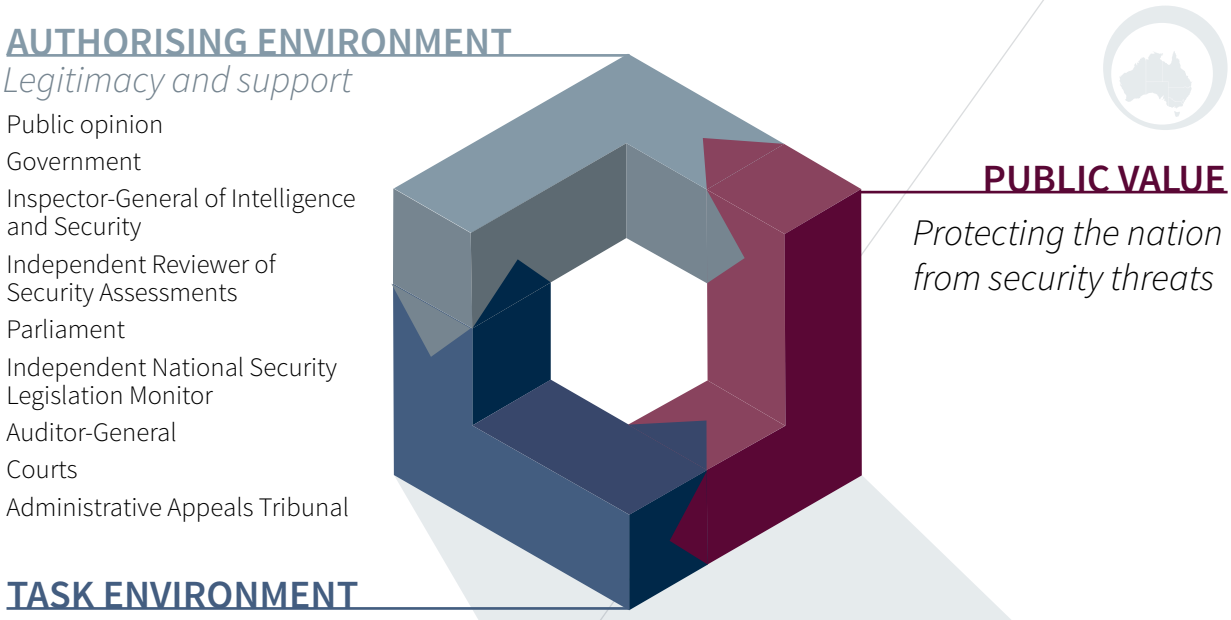
Our role in supporting all Australian governments and agencies (both Commonwealth and State/Territory) protect Australia from security threats means we have a complex operating environment.

We deploy our unique capabilities to protect Australia and also rely on the support of people from all communities, Australian and international intelligence, law enforcement, and security agencies, and business and industry.

We have a rich authorising environment of stakeholders who provide legitimacy and support for our activities. This reflects Australia's approach of intelligence agencies being accountable to the people through legislation, parliamentary oversight, ministerial accountability and guidelines, and independent oversight by the Inspector-General of Intelligence and Security. These arangements are designed to be as public as possible, but some elements must be conducted in private.

Figure 1 shows the relationship between the public value we provide, the task environment our activities are conducted within, and the authorising environment that provides us with legitimacy and support.[4]

FIGURE 1 ASIO's public value and partnerships



[4] This figure is an application of the strategic triangle described by M.H. Moore in *Creating Public Value: Strategic Management in Government*, Harvard University Press.

Australia's security environment over 2016–17 to 2019–20

Australia's security environment arises out of the interaction between our national interests and threats that could potentially harm those interests. The sources of threats to Australia's security out to 2020 will continue to be volatile and defined primarily by Islamist terrorism, hostile espionage and interference activities and malicious cyber activities.



- The counter-terrorism challenge Australia faces is underscored by events: since the national terrorism threat level was raised in September 2014, there have been three attacks and ASIO and law enforcement partners have engaged in nine disruption operations in response to imminent attack planning in Australia.

  These events speak to the enduring nature of the extremism challenge Australia faces, with the conflicts in Syria and Iraq having energised local extremists in a way no other terrorism arena has. This has had the effect of dropping the threshold for violence and means jihadism in Australia is more self-sustaining than previously.



- Clandestine foreign actors are causing harm to Australia through espionage, interference and cyber activity that seeks to undermine our political and economic sovereignty.

  We continue to work with our partners on detecting, defending and degrading the activities of these actors. However, such activities are inherently difficult to detect, including in the cyber realm, and can carry consequences that may not be realised for decades.

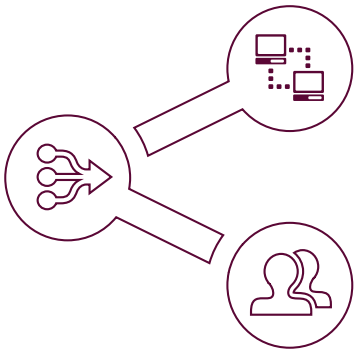
  The gap is likely widening between the scale and scope of harm experienced to Australia's sovereignty, government and defence systems, and commercial and intellectual property, and our ability to successfully mitigate that harm.



- Our border security focus will continue to be on partnering with the Department of Immigration and Border Protection, including supporting the delivery of the annual migration program (with a particular focus in 2016–17 on the additional 12,000 places allocated to Syrian refugees) and in support of the Department's citizenship functions.

  We will continue to collaborate with the Department to manage downstream security risks associated with flows of people seeking entry to Australia and applying for citizenship. There will be some complex cases, including ones where we recommend against travel, entry, or citizenship on security grounds.

Challenges to ASIO's activities over 2016–17 to 2019–20



Public debate about national security will continue to evolve and this is a healthy feature of a democracy. In an environment of declining government revenue and multiple calls on the public purse it is natural for national security expenditure to be closely scrutinised and challenged. We will need to ensure our message is understood so that stakeholders continue to appreciate the nature of threats and the capabilities required to counter them, and to ensure security fatigue does not develop in Australian society.

Due to the dynamic nature of the security environment, we anticipate that demand across government for our products and services will continue to outpace supply, requiring us to continue to prioritise and manage expectations. We will continue to have a major role to play in delivering intelligence and advice to shape Australia's security system and overall approaches to countering sources of threat and reducing harm to the national interest. Key areas of increasing demand will likely include:

- the national security implications of foreign investment
- telecommunications sector security
- security threats to the Australian defence industry
- protection of critical infrastructure
- ongoing protective security measures to mitigate terrorism.

We anticipate some challenges which will persist over the life of this plan relating to the development of multiple intelligence capabilities:

- The recruitment and retention of skilled knowledge workers
- The continued high demand for human intelligence skills
- The diminishing value from increasingly encrypted content and datasets
- The need for big data analytics to manage an increasing variety, velocity and volume of data, and the related information management adaptation.

These ongoing capability challenges will require internal reform and the development of new operational paradigms.

We will need to continue to effectively partner with Australian agencies and consider how we can best use our strengths in concert with others to achieve security outcomes for Australia.

A key strength we have is our anticipatory intelligence work across operations, analysis and advice to government. We will leverage this strength to deploy strategic security layers that provide early warning of possible threats and assist us manage emergent risks. Such strategic layers already include the National Security Hotline, engagement with owners of national critical infrastructure, security assessment regimes, and advice in relation to security aspects of foreign investment.

Performance

We pursue our purpose through five activities. The following pages relate each activity to its intended result, delivery strategies, performance measures and targets.

The overall approach to performance measurement is to set measures in terms of the effects generated for Australian governments, agencies, business, and industry by our security advice, reporting, and services. The same measures and targets will be applied over 2016–17 to 2019–20. We will report our performance annually through the Annual Performance Statements included in our annual report.

We are also subject to a range of external evaluations of our intelligence role. These include: the Department of the Prime Minister and Cabinet's annual performance review of the Australian Intelligence Community; the evaluation processes established as part of the Australian Government's strengthened counter-terrorism governance arrangements in 2014; and the Office of National Assessments-chaired National Intelligence Collection Management Committee's ongoing evaluation of national intelligence collection efforts.

INTENDED RESULTS

- We conduct our activities in a safe and secure way to protect our people, capabilities, and assets.
- We conduct our activities in accordance with the law, ministerial guidelines, community expectations.

PERFORMANCE MEASURE

The safety of our staff is maintained.	Legality and propriety of our activities and effectiveness of our engagement with oversight and accountability bodies.	The security of our activities.
TARGETS		
Our senior leaders continue to be exemplars and to drive a work culture, systems, and individual conduct which promote officer safety. We maintain high levels of work, health, and safety capacity and ongoing training of staff.	Our senior leaders continue to be exemplars and to drive a work culture, systems, and individual conduct which are legal, ethical, and respect human rights. We proactively engage with oversight and accountability bodies and provide as much information as possible for use in the public domain.	Our senior leaders continue to be exemplars and to drive a work culture, systems, and individual conduct which embody security. We continue to meet the requirements of the Australian Government's Protective Security Policy Framework.

To protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for Government, government agencies, and business

Activities



Countering terrorism and the promotion of communal violence



Countering espionage, foreign interference and malicious insiders



Countering serious threats to Australia's border integrity



Providing protective security advice to government and business



Collecting foreign intelligence in Australia

ASIO will deliver intelligence and advice on security matters to Commonwealth, state and territory governments, to law enforcement, border and national security agencies, and to Australian businesses. Collaboration with these stakeholders also contributes to ASIO's work by providing intelligence policy settings, agency capabilities and information flows.

Partners are a significant source of information and expertise

We directly engage with partners and consider the effects of our advice

INTENDED RESULTS

We provide partners with actionable intelligence, advice, and services

We use our unique assets to support partners achieve their outcomes

We will measure success through

Effective identification of threats to Australia's security

Effective advice, reporting, and services

Effective partnering

Countering terrorism and the promotion of communal violence



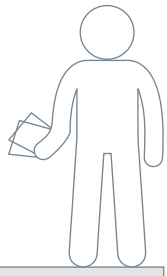
INTENDED RESULTS

- We identify terrorism-related activities and the promotion of communal violence affecting Australia, its people and its interests.
- We provide advice and undertake or enable activities that disrupts terrorism-related activities and the promotion of communal violence affecting Australia, its people and its interests.
- Our advice improves the effectiveness of the Australian Government's protective security responses to terrorism.
- Our advice supports the development of Australian Government policy responses to terrorism and the promotion of communal violence.

PERFORMANCE MEASURE

We effectively identify and investigate threats to Australia's security.	We provide effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security.	We work effectively with partners to generate tangible counter-terrorism effects for Australia and partner countries.
TARGETS		
New security leads are identified and consistently prioritised and pursued.	The Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice.	Partners can readily access our intelligence.
Security assessment regimes enable action by other agencies to prevent security risks to Australia.	Law enforcement, border and other national security partners use our advice to manage and disrupt security risks.	Partners view joint operations with us as an effective way to achieve shared outcomes.
	Business and industry adopt our security advice and are satisfied with their engagement.	National security partners use our advice to disrupt travel of Australians or locally-based support for terrorism overseas.

Countering espionage, foreign interference and malicious insiders



INTENDED RESULTS

- We discover espionage, foreign interference and the activities of 'malicious insiders' and degrade their impacts.
- Our advice improves the effectiveness of Australian Government defences against clandestine espionage, foreign interference and malicious insiders.

PERFORMANCE MEASURE

We effectively identify and investigate threats to Australia's security.	We provide effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security.	We work effectively with partners to counter clandestine foreign activity.
TARGETS		
New security leads are identified and consistently prioritised and pursued.	The Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice.	Partners can readily access our intelligence.
Security assessment regimes enable action by other agencies to prevent security risks to Australia.	Law enforcement, border and other national security partners use our advice to manage and disrupt security risks. Business and industry adopt our security advice and are satisfied with their engagement.	Partners view joint operations with us as an effective way to achieve shared outcomes.

Countering serious threats to Australia's border integrity



INTENDED RESULTS

- We identify activities that represent a serious threat to Australia's border integrity.
- Our advice is used to assist Australia's border agencies effectively manage and/or disrupt activities that represent a serious threat to Australia's border integrity.

PERFORMANCE MEASURE

We effectively identify and assess threats to Australia's security.	We provide effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security.	We support DIBP meet its migration program and refugee and humanitarian resettlement goals.

TARGETS

New security leads are identified and consistently prioritised and pursued.	The Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice.	Security advice to DIBP is timely and meets the agreed Service Level Agreements and is responsive to DIBP's other priorities.
Security assessment regimes enable action by other agencies to prevent security risks to Australia.	Law enforcement, border and other national security partners use our advice to manage and disrupt security risks.	

Providing protective security advice to government and business



INTENDED RESULTS

- Government, business, and industry adopt security by design to protect Australia's people, assets, and other national interests.
- There is increased protective security awareness and capacity across Australian Government agencies, business, and industry.

PERFORMANCE MEASURE

We provide effective protective security advice, reporting and services that inform security by design by government, business, and industry.

TARGETS

Our expertise and advice informs security policies and approaches within government agencies, business, and industry.

Protective security resources are directed at protecting the assets, infrastructure and systems judged by us to be most at risk.

The annual program of physical security certifications is achieved.

Collecting foreign intelligence in Australia



INTENDED RESULTS

- We provide niche foreign intelligence collection services to partners, in accordance with National Intelligence Priorities.

PERFORMANCE MEASURE

We provide intelligence that is useful to progress Australia's national security, foreign relations, or economic wellbeing.

TARGETS

We are responsive to the requirements and interests of clients.

Strategic Plans

We have in place strategic plans for 2016–17 for our activities of countering terrorism, and countering espionage and foreign interference. These plans cascade from this corporate plan and identify areas of focus, specific goals, delivery strategies, and intended outcomes. More detailed business plans cascade from these strategic plans.

The **Counter Terrorism strategic plan** is designed around three areas of focus:

Enhance

- Augment collection, analysis, assessment and advice capabilities to build the teams we need in the current and future security environment and keep us ahead of the counter-terrorism threat

Innovate

- Identify new capabilities and reform business practices to use resources more effectively

Influence

- Counter-terrorism decision-making by the Australian Government and other partners is informed by our knowledge, advice and expertise
- Our capabilities are more efficiently integrated with those of our partners and deliver optimum outcomes

The **Counter Espionage and Interference strategic plan** is based on four pillars: the integrated work programs designed to Discover, Defend against, and Degrade threats from hostile state actors, and the work to Build the capability of our people, teams, and partnerships.

Discover

- Use all lawful sources and methods to understand the intent and capability of our adversaries
- Develop authoritative understanding of threats
- Identify and understand our vulnerabilities in order to shape the environment

Defend

- Investigate highest harm activity and provide accurate and comprehensive security assessments to help assure the integrity of government, business and security of critical infrastructure
- Share understanding of threats to raise awareness and build partnerships which help counter the threats

Degrade

- Act judiciously, in concert with partners, to diminish the capacity of foreign adversaries to harm Australia
- Help shape the environment to make it harder for adversaries and malicious actors to achieve their objectives

Build

- Build talent through enhanced people performance – leadership, teams and individuals
- Ensure our systems, practices and procedures are counter intelligence aware
- Leverage our partnerships to greatest effect

Capability

ASIO2020



In response to the issues discussed in the Environment section, on 1 July 2016 we embarked on the ASIO2020 program to address the most significant challenges to our future success. ASIO2020 has four strands of work that set our strategic capability agenda and goals for the next four years:

Context – *our authorising and task environments*

A compelling value proposition will ensure we maximise our contribution to society and therefore enjoy continued public support, authority and resources. We need to have our value understood by our society, government, and partners. We also need to focus on what we can best offer to partners so we are recognised as their national security partner of choice.

Culture – *the backbone to our success*

A positive work culture will drive our productivity and contribute to the organisation being an employer of choice. We need to enable a culture of innovation and diversity and unlock the benefits for our work. We also need to promote a single organisational vision while recognising the validity of different business models.

People – *our most important asset*

Our workforce is our core asset in a competitive labour market. In order to succeed we must obtain maximum benefit from our people within a frame of mutual obligation. Strong and flexible human resources management approaches consistently applied will lift our value proposition for attracting, recruiting, and retaining the people we need in the future.

Systems – *How we work (our practices, tools, and mindsets)*

Work systems and mindsets that are fit for purpose, can adapt to change, and support a data discovery approach will enable us to learn and manage tomorrow's security challenges. We need to address the data discovery challenge to reduce our information liability, obtain more breathing space from adversaries, and work with partners to share risk and opportunities.

An agile development approach is being taken to develop the projects within each strand in consultation with our workforce.

Partnerships

The Australian people will continue to be our prime partner enabling our success. We will continue to engage publicly through speeches, attendance at community functions, and appearances in the media.

We also work with law enforcement, border and national security agencies in the Commonwealth and the states and territories. This collaboration contributes to achieving our purpose by providing us with intelligence policy settings, agency capabilities and information flows. We contribute to the outcomes of other agencies through security advice, intelligence and services. Our key partner agencies will continue to be Australia's intelligence and law enforcement agencies, our policy counterparts, and cooperating agencies of allied and friendly governments.

Resourcing

We continue to build our capacity to counter terrorism through the resourcing provided under the *National Security—additional counter-terrorism funding* measure announced in the 2014–15 Mid-Year Economic and Fiscal Outlook (MYEFO). During 2016–17, our focus to implement this measure will continue to be on:

- recruiting and retaining skilled people across assessment, investigation and analysis, human intelligence and technical collection, and operational support teams
- capital investment in technical capabilities.

Risk oversight and management

Engaging with risk is central to our purpose and activities. Our approach to understanding risk is driven by a dynamic operating environment, incomplete information, and a variety of threat sources. This, demands a tailored approach incorporating:

- An appreciation by our people that risk is everyone's responsibility.
- A sound appreciation of our key strategic objectives within our operating environment.
- Thoughtful risk-taking based on sound, informed and consistent risk decision-making.
- Identification of different types of risk and their management.

ASIO's overall approach to risk is anticipated to remain the same over the next four years.

Our risk management approach places risks across our business and at all levels into three categories[5]:

PREVENTABLE RISKS
"risks not to be taken"
STRATEGY RISKS
"risks that may be worth taking"
EXTERNAL RISKS
"risks to be planned for"

We use an enterprise risk landscape to capture our risks and our approach to:

- describing our risk appetite and threshold;
- relating overall risk objectives to our activities;
- defining enterprise risks relating to our authorising environment and task environment; and
- assigning responsibility within our governance system for managing the risks (see pages 25–27).[6]

Our governance committees have a key role in identifying risk trends and developments, reviewing risk levels, considering management strategies, and determining action (see pages 25–27). The Executive Board has a key role in advising the Director-General and uses performance and risk information to adjust our risk settings.

We apply this risk philosophy to our core intelligence work, including in prioritising operational resources devoted to countering terrorism, espionage and foreign interference, and threats to the border at a strategic and tactical level. The prioritisation is intelligence led and relies on judgments being made about likelihood and the potential damage activities could lead to. The highest priority cases demand the greatest intelligence response.

We continue to refine our risk management and performance frameworks in an environment where adversaries consciously seek to avoid detection and learn from their experiences and those of others, and where the harm to Australia's security may be latent and not immediately manifest.

5 After the approach described by R.S. Kaplan and A. Mikes, 'Managing Risks: A New Framework', Harvard Business Review, June 2012

6 The detail of the landscape is classified and has been removed from the public version of the corporate plan.

Review of ASIO Risk Management Framework
ASIO's Audit and Risk Committee

Ad hoc referrals

Enterprise Risk Management
By ASIO's Executive Board

Review of Enterprise Risks
On a regular basis the corporate committees will review ASIO's risk landscape.

Enterprise Risk Analysis and Coordination
Provides analysis of committee risk reports and consequential evaluation of ASIO's risk landscape.

Enterprise Risk Reports
The Executive board will delegate the management of some risks to ASIO corporate committees.

Committees will also provide advice on ASIO's risk policies, processes, systems and training as appropriate.

Review of identified risks
ASIO corporate committees will review risks according to their portfolio.

Each corporate committee will issue a risk threshold statement for Executive board endorsement.

Risk identification
Work areas and business processes will assist in risk identification (e.g. Divisional and Branch business plans, Quarterly Performance Reports).

