



Australian Government

Australian Security
Intelligence Organisation

Corporate Plan 2018–19



© Commonwealth of Australia 2018

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

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

<i>DIRECTOR-GENERAL'S INTRODUCTION</i>	<i>1</i>
<i>PART 1: ASIO'S PURPOSE</i>	<i>2</i>
<i>PART 2: SECURITY AND OPERATING ENVIRONMENT</i>	<i>4</i>
<i>PART 3: PERFORMANCE</i>	<i>7</i>
<i>PART 4: CAPABILITY</i>	<i>14</i>
<i>PART 5: RISK OVERSIGHT AND MANAGEMENT</i>	<i>17</i>



Duncan Lewis AO DSC CSC

Director-General of Security



Peter Vickery

Deputy Director-General
Operational Support
and Capability Group



Heather Cook

Deputy Director-General
Operations and
Assessments Group



Wendy Southern PSM

Deputy Director-General
Strategic Enterprise
Management Group

Director-General's introduction

I am pleased to present the 2018–19 *Australian Security Intelligence Organisation (ASIO) corporate plan*, which covers the period of 2018–19 to 2021–22 as required under paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

Australia continues to face a challenging security and operating environment. Terrorism remains a significant threat across the world. Despite Islamic State of Iraq and the Levant's (ISIL) military losses in Syria and Iraq, ISIL and other extremist groups will continue to pose a threat to Australia and our interests globally and at home. Espionage and foreign interference targeting Australia are also occurring on an unprecedented scale and represent a serious threat to Australia's sovereignty, security and prosperity.

Throughout the period of this plan, ASIO will work to protect Australia, its people and its interests from these threats by collecting and assessing security intelligence, and by providing advice to national security partners to assist them in managing security risks and disrupting harmful activities.

ASIO does not, and cannot, do this work alone. An effective response to the security challenges facing Australia requires strong partnerships among federal, state and territory governments; national security and law enforcement agencies; industry; academia; and Australia's international partners. The recent establishment of the Department of Home Affairs and the Office of National Intelligence presents new opportunities to strengthen our cooperation with national security partner agencies and to enhance the nation's intelligence and security capabilities. I look forward to working closely with these organisations and our other national and international security partners.

Within ASIO, we have commenced a major transformation to ensure the Organisation remains fit for purpose in the increasingly complex security and operating environment. In 2017, I commissioned an external review of our approach to the use of technology, as well as the relationships between technology and our approach to people, culture and collaboration. The report from this review,

A digital transformation of the Australian Security Intelligence Organisation, recommended that we change our business model to capitalise on the benefits of augmented decision-making and data science.

The successful transformation of ASIO into an organisation with world-class digital capability will be among my highest priorities during the period of this plan and beyond.

This corporate plan includes five parts:

- ▶ **Part 1** outlines ASIO's purpose and values.
- ▶ **Part 2** describes the security threats and operating challenges we will face as we work with our national security partners.
- ▶ **Part 3** describes our priorities and outlines our performance framework—the measures we will use to assess how well we have achieved our purpose.
- ▶ **Part 4** provides an overview of how we are building the capabilities we need to achieve our purpose in a digitally connected world.
- ▶ **Part 5** describes our approach to the management and oversight of risk.

Duncan Lewis AO DSC CSC

Director-General of Security

Part 1: 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.

Our work is anticipatory. We seek to identify, investigate and assess potential security threats, and work with 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.

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



countering terrorism



countering espionage, foreign interference, sabotage and malicious insiders



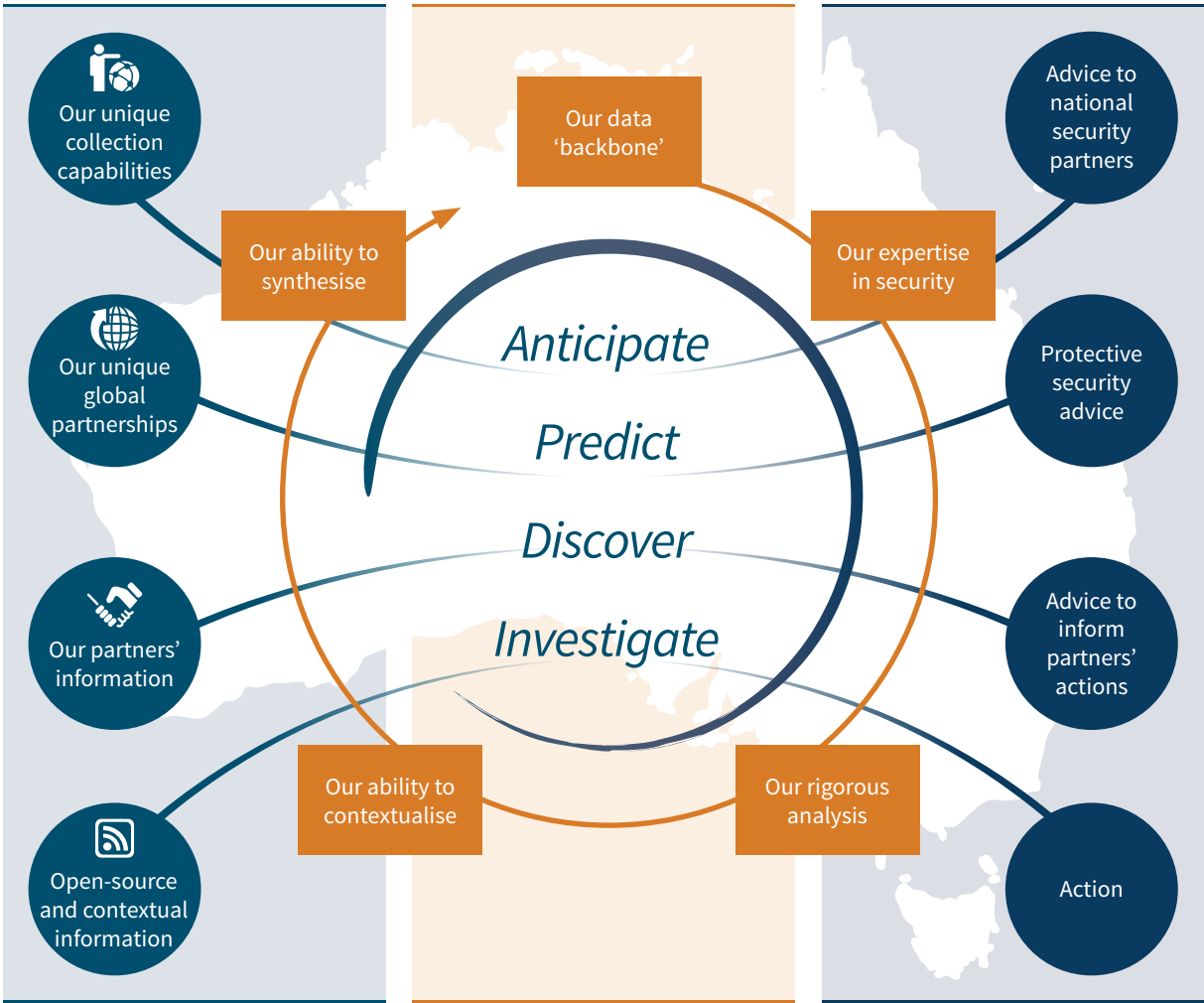
countering serious threats to Australia's border integrity



providing protective security advice to national security partners

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



1

Part 2: security and operating environment

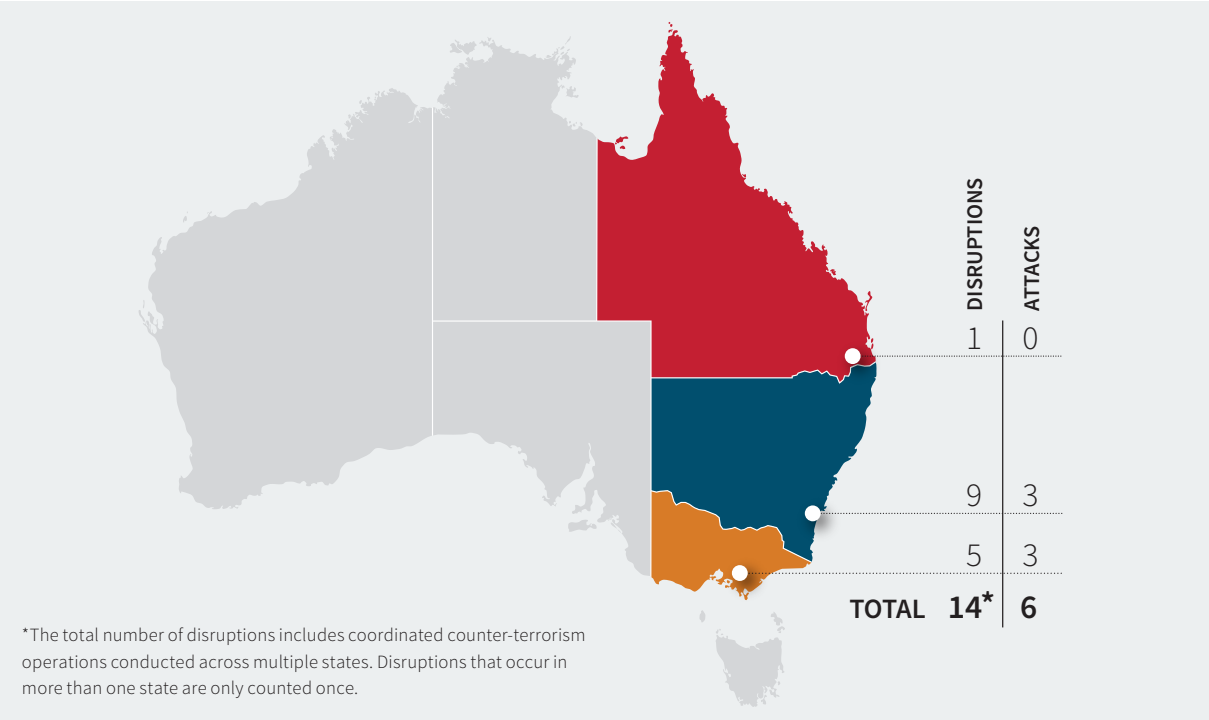
The key factors affecting our security and operating environment are likely to persist over the four-year period of this plan.

Violent extremism remains a serious security issue globally and within Australia. Since the national terrorism threat level was raised in September 2014, there have been six onshore terrorist attacks targeting people.

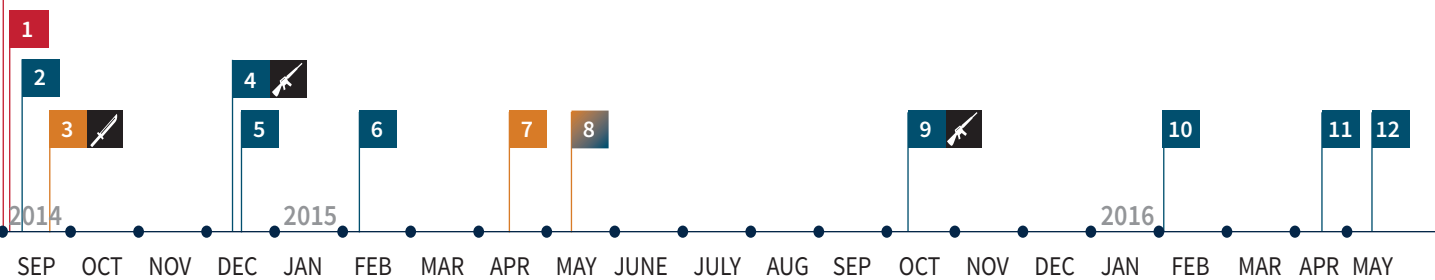
Fourteen planned terrorist attacks in Australia have been disrupted. The conflict in Syria and Iraq has shaped this generation of Australian extremists—diverse in age, gender and ethnicity—who will present an enduring security risk. Foreign fighters returning or forcibly dispersed from Syria and Iraq are also a long-term risk to Australia, its people and its interests at home, in our immediate region and overseas.

The national terrorism threat level for Australia is currently **PROBABLE**—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct a terrorist attack in Australia.



Onshore terrorist attacks and counter-terrorism disruptions since September 2014




National terrorism threat level raised in September 2014




2014

- 1 OP BOLTON 10 SEP** Preparation for an onshore attack disrupted.
- 2 OP APPLEBY 18 SEP** Preparation for an onshore attack disrupted.
- 3 OP GOODRICH 23 SEP** Two police officers attacked.  Assailant killed.
- 4 OP ARRABELLA 15 DEC** Martin Place siege.  Three killed including assailant.
- 5 OP APPLEBY 18 DEC** Possible plot against government buildings disrupted.


2015

- 6 OP CASTRUM 10 FEB** Possible plot to target members of the public disrupted.
- 7 OP RISING 18 APR** Possible plot against Anzac Day services or police disrupted.
- 8 OP AMBERD KASTEEL 8 MAY** Coordinated raids disrupt possible onshore attack planning.
- 9 OP SF FELLOWS 2 OCT** NSW Police Force civilian employee killed.  Assailant killed.


2016

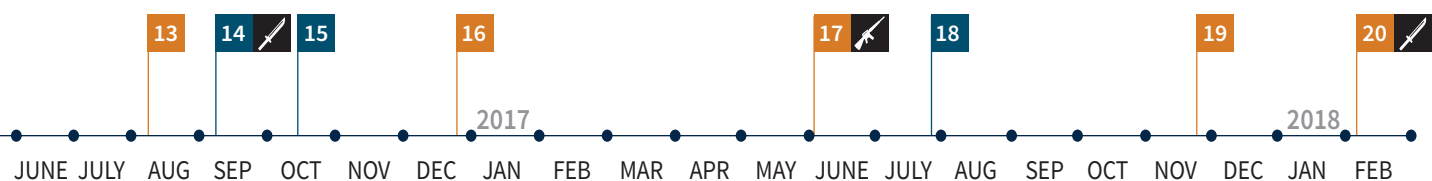
- 10 OP CHILLON JAN/FEB** Possible plot disrupted.
- 11 OP VIANDEN 24 APR** Possible plot against Anzac Day services disrupted.
- 12 OP SANANDRES 17 MAY** Possible plot disrupted.
- 13 OP FORTALEZA 6 AUG** Alleged preparation for plot by an extreme right-wing individual disrupted.
- 14 OP TRESSIDER 10 SEP** Stabbing attack against a member of the public.  Assailant arrested.
- 15 OP RESTORMEL 12 OCT** Possible plot disrupted. Two individuals arrested carrying knives.
- 16 OP KASTELHOLM 22 DEC** Possible plot disrupted. Four individuals charged with acts done in preparation for a terrorist act.

2017

- 17 OP TEMATIN 5 JUNE** Member of the public killed and three police officers injured during siege/hostage attack.  Assailant killed.
- 18 OP SILVES 29 JULY** Alleged plot against aviation disrupted. Two individuals charged with terrorism offences.
- 19 OP SAN JOSE 27 NOV** Alleged New Year's Eve plot disrupted. One individual charged with terrorism offences.

2018

- 20 OP VECCHIO 9 FEB** Knife attack against a member of the public in their home.  Assailant was arrested and charged with a terrorism offence.



Espionage and foreign interference directed against Australia is occurring at an unprecedented level. Foreign actors are aggressively seeking access to privileged and classified information on Australia’s alliances and partnerships; position on international diplomatic, economic and military issues; energy and mineral resources; and innovations in science and technology. They are also attempting to clandestinely influence the opinions of members of the Australian public and media, Australian Government officials, and members of Australia-based diaspora communities.

In this environment of heightened security threats with complex and resource-intensive operating demands, the requirement of our national security partners for timely intelligence and reliable protective security advice is increasing. ASIO will continue to work with our national security partners to protect Australians and Australia’s interests from the security threats facing the nation.

- **Part 3** of this corporate plan describes our priorities and the measures we will use to assess our performance and how well we have achieved our purpose.

The evolving technological landscape

Rapidly changing and diversifying technology is increasing the complexity of the environment in which we operate. These advances present us with both opportunities and challenges.

The ‘internet of things’ is changing how people live, work and operate. It is increasing the variety, volume and velocity of digital information and changing how ASIO operates. Technology is also providing individuals and groups who are engaged in harmful activities a greater range of means—assisting them to hide their activities from security and law enforcement agencies, and to uncover our activities and capabilities.

Along with our national security partners, we will remain under considerable pressure to develop and maintain technological and other capabilities to access and analyse information required to identify and disrupt these harmful activities.

- **Part 4** of this plan provides an overview of how we are building the capabilities we need to achieve our purpose in a digitally connected world.



Part 3: performance

ASIO's 2018–19 Performance Framework connects directly to our purpose: to protect Australia, its people and its interests from threats to security through intelligence collection and assessment, and the provision of advice to our national security partners.

For the period of this plan, 2018–19 to 2021–22, we will work to achieve our purpose through four key activities that focus on:

- ▶ countering terrorism;
- ▶ countering espionage, foreign interference, sabotage and malicious insiders;
- ▶ countering serious threats to Australia's border integrity; and
- ▶ providing protective security advice to national security partners.

Our performance framework describes the measures we will use to assess our achievements. The key activity tables on pages 10 to 13 provide a summary of each activity, and describe high-level risks to achieving them, and how we intend to mitigate those risks.

These performance measures align with the performance criterion set out in ASIO's 2018–19 portfolio budget statement (PBS): *Advice that assists the Australian Government and ASIO partners to manage security risks and disrupt activities that threaten Australia's security*. Our performance reporting against these corporate plan measures will address the 2018–19 PBS performance criterion.

ASIO 2018–19 Performance Framework summary

3	PERFORMANCE MEASURES	KEY ACTIVITIES	1	2	3	4
			Countering terrorism	Countering espionage, foreign interference, sabotage and malicious insiders	Countering serious threats to Australia's border integrity	Providing protective security advice to national security partners
			A Our advice informs Australian Government policy development and responses to terrorism.	Our advice informs Australian Government policy development and responses to espionage, foreign interference, sabotage and malicious insiders.	Our advice informs Australian Government policy development and responses to serious threats to Australia's border integrity.	Our protective security advice and services assist national security partners to manage security risks.
			B National security partners use our advice to disrupt and defend against terrorism.	National security partners use our advice to disrupt and defend against harmful espionage, foreign interference, sabotage and malicious insiders.	National security partners use our advice to disrupt and defend against serious threats to Australia's border integrity.	
			C	We collect foreign intelligence in Australia that advances Australia's national security interests.		

Performance assessment, reporting and assurance

We will measure and assess our performance by reviewing on a tri-annual basis:

- ▶ independent intelligence and national security community evaluations;
- ▶ stakeholder feedback; and
- ▶ performance against service-level agreements with relevant agencies.

We will also conduct an annual survey of our senior stakeholders in federal, state and territory governments; national security partners and industry. This survey will supplement feedback collected from stakeholders throughout the year and inform development of the annual performance statement, contained in ASIO's annual report to parliament.

ASIO performance reporting cycle¹

ASIO corporate plan 2018–19	Tri-annual performance reporting	PBS 2019–20: performance forecast	Annual performance statement 2018–19	Annual report 2018–19
Set performance objectives	Monitor performance	Forecast performance	Report on performance	Publish report on performance
Corporate plan key activities and performance measures endorsed by Executive Board and approved by Director-General.	Intelligence Committee monitors key activity performance throughout year, reporting tri-annually to the Executive Board.	PBS performance forecast drawn from tri-annual reports for November 2018 and March 2019.	Annual performance statement drawn from tri-annual reports for November 2018, March 2019 and June 2019 and annual stakeholder survey.	Annual performance statement published in ASIO annual report to Parliament 2018–19.
Performance objectives incorporated into divisional business plans.	Tri-annual performance reports provided to Executive Board in November 2018, March 2019 and June 2019.	Forecast endorsed by Executive Board and approved by Director-General.	Endorsed by Executive Board and approved by Director-General.	Annual report to be provided to Minister by 15 October 2019 for tabling in Parliament.
Plan commences operation on 1 July 2018.		PBS published with Budget (early May 2019).	Produced as soon as practicable at the end of 2018–19 reporting period.	
The Audit and Risk Committee reviews and provides advice to the Director-General on the appropriateness of ASIO's corporate plan performance measures, tri-annual performance reports, PBS performance forecast and annual performance statement.				

¹ 2018–19 dates are indicative. This cycle will apply to each year covered for the four year period of this plan.

1 Key activity 1: countering terrorism

PERFORMANCE MEASURES

Measure 1A: our advice informs Australian Government policy development and responses to terrorism

Our priorities will include:

- ▶ supporting the development of national policies and legislative reforms that protect Australia, its people and its interests from terrorism; and
- ▶ enhancing our Australian Government partners’ understanding of Australia’s terrorism-related threat environment.

Measure 1B: national security partners use our advice to disrupt and defend against terrorism

Our priorities will include:

- ▶ contributing to the disruption of terrorist threats from individuals and groups;
- ▶ supporting the prosecution of individuals for terrorism and related offences; and
- ▶ assisting partners to implement measures to mitigate terrorism-related risks, including through threat assessments that inform the establishment of ‘declared areas’, the proscription of extremist groups, the Department of Foreign Affairs and Trade’s travel advisories, and strategies for securing special events and at-risk public places.

RISKS TO PERFORMANCE

Risk	Mitigation
Heightened threat environment: the volume of terrorism-related activity exceeds our capacities, reducing the effectiveness of our advice.	Rigorous prioritisation of effort focusing on activities representing the greatest potential harm. Collaboration with national security partners on the prioritisation of and responses to threats. Implementation of robust ‘discovery’ processes to identify new and emerging threats.
Insufficient capability: rapid changes in the technological and operating environments reduce our ability to identify threats, limiting the effectiveness of our advice.	Implementation of ASIO’s transformation objectives (see Part 4 of this plan). Collaboration with national security partners on capability development.
Ineffective partnering: our advice does not meet the requirements of partners and does not assist them to respond effectively to threats.	Close and regular engagement with partners on their specific requirements.

2 Key activity 2: countering espionage, foreign interference, sabotage and malicious insiders

PERFORMANCE MEASURES

Measure 2A: our advice informs Australian Government policy development and responses to espionage, foreign interference, sabotage and malicious insiders

Our priorities will include:

- ▶ continuing to broaden Australian Government understanding of the risk of harm from espionage, foreign interference, sabotage and malicious insiders;
- ▶ supporting the development and implementation of Australian Government strategy to counter foreign interference; and
- ▶ supporting the development of Australian Government responses to mitigate security threats to critical infrastructure, sensitive data and emerging technologies.

Measure 2B: national security partners use our advice to disrupt and defend against espionage, foreign interference, sabotage and malicious insiders

Our priorities will include:

- ▶ contributing to the disruption of espionage and foreign interference threats;
- ▶ supporting the prosecution of individuals for espionage and foreign interference-related offences;
- ▶ assisting the Department of Defence and defence industry to secure Australia's defence capabilities; and
- ▶ assisting partners, through our personnel security assessments, to protect classified and sensitive government information, areas and resources.

Measure 2C: we collect foreign intelligence in Australia that advances Australia's national security interests

Our priorities will include collecting intelligence that assists Australia's foreign intelligence agencies.

RISKS TO PERFORMANCE

Risk	Mitigation
Heightened threat environment: the scale of espionage and foreign interference activity exceeds our capacities, reducing the effectiveness of our advice.	Rigorous prioritisation of effort focusing on activities representing the greatest potential harm. Collaboration with national security partners on prioritisation of and responses to threats.
Insufficient capability: the sophisticated capabilities of hostile actors reduce our ability to identify harmful activity, limiting the effectiveness of our advice.	Implementation of ASIO's transformation objectives (see Part 4 of this plan). Collaboration with national security partners on capability development.
Ineffective partnering: our intelligence and advice does not reach the right people and does not assist them to respond effectively to threats.	Implementation of a more effective, tailored outreach program. Close and regular engagement with partners on their specific requirements.

3 Key activity 3: countering serious threats to Australia’s border integrity

PERFORMANCE MEASURES

Measure 3A: our advice informs Australian Government policy development and responses to serious threats to Australia’s border integrity

Our priorities will include providing advice to support development of national policies and legislative reforms that protect Australia, its people and its interests from serious threats to our border integrity.

Measure 3B: national security partners use our advice to disrupt and defend against serious threats to Australia’s border integrity

Our priorities will include:

- ▶ assisting Operation Sovereign Borders partners to identify and disrupt people-smuggling ventures;
- ▶ supporting the integrity of our border by providing advice to Home Affairs, through our security assessments on individuals of security concern who are applying for Australian visas or citizenship; and
- ▶ assisting national security partners, through our access security assessments, to prevent individuals of concern from accessing security-sensitive areas or substances.

RISKS TO PERFORMANCE

Risk	Mitigation
Heightened threat environment: the volume and complexity of visa, citizenship and access security referrals, and people-smuggling ventures exceeds our capacities, reducing the effectiveness of our advice.	<p>Prioritisation of assessment effort focusing on activities representing the greatest potential harm, while simultaneously recognising the effect any potential delay in our assessments may have on the lives and livelihoods of individuals.</p> <p>Working with national security partners on prioritisation of caseloads to meet broader government objectives.</p>
Insufficient capability: rapid changes in the technological and operating environments reduce our ability to provide timely, actionable advice to our partners, limiting the effectiveness of our advice.	<p>Implementation of ASIO’s transformation objectives (see Part 4 of this plan).</p> <p>Collaboration with national security partners on capability development.</p>
Ineffective partnering: our advice does not meet the requirements of partners and does not assist them to respond effectively to threats.	<p>Close and regular engagement with partners on their specific requirements.</p>

4 Key activity 4: providing protective security advice to national security partners

PERFORMANCE MEASURES

Measure 4A: our protective security advice and services assist national security partners to manage security risks

Our priorities will include:

- ▶ developing protective security guidance material;
- ▶ assessing security zones for certification;
- ▶ delivering specialist protective security training;
- ▶ evaluating security equipment and construction methods; and
- ▶ providing technical surveillance counter measures inspections.

RISKS TO PERFORMANCE

Risk	Mitigation
Heightened threat environment: the volume of demand for protective security advice exceeds our capacities, reducing the accessibility of our advice.	Rigorous, intelligence-led prioritisation of effort focusing on activities benefiting those most at risk, and those representing the broadest benefit.
Insufficient capability: rapid changes in the technological and operating environments reduce our ability to identify threats, limiting the effectiveness of our advice.	Implementation of ASIO's transformation objectives (see Part 4 of this plan). Collaboration with national security partners to enhance the protective security capability within Australia.
Ineffective partnering: our advice or services do not meet the requirements of partners and does not assist them to respond effectively to threats.	Close and regular engagement with partners on their specific requirements.

3

Part 4: capability

To achieve our purpose in a challenging environment of heightened security threats with complex and resource-intensive operating demands, we will need to continuously review and strengthen our capabilities over the four-year period of this plan.

The 2017 digital transformation review, commissioned by the Director-General as part of the ASIO 2020 organisational reform program, found we need to enhance our ability to collect, manage and analyse data, and transform our approach to technology and how we do business. The review made recommendations on ASIO's approach to technology, people, culture and collaboration.

We have commenced implementing the recommendations of the review.

Technology

Technology is now a part of everyday life for all members of our community; we are living, working and communicating in a digitally connected world. Individuals and groups posing threats to Australia's security have ready access to sophisticated technology, which presents unprecedented challenges to intelligence collection and analysis efforts. Understanding the uses and inherent vulnerabilities of technology is crucial to our ability to successfully defend Australia's security.

Emerging technologies provide ASIO with new tools and techniques that we can employ in responding to Australia's security challenges. We will position ourselves to successfully employ augmented decision-making and artificial intelligence processes to protect our nation and its interests from threats to security.

4



People

People continue to be our most important asset. In a competitive labour market, talented individuals are in demand—people who can operate effectively across our human intelligence, technology, surveillance, investigative, assessment, legal and corporate areas.

We are using the findings from the 2017 digital transformation review to refine our recruitment, career management and training frameworks in order to attract and develop talented people, provide rewarding career opportunities, and build our workforce of the future.



4

Culture

To continue delivering our objectives on this path of digital transformation, ASIO’s culture needs to be grounded in strong leadership with a focus on technology and data.

Our leadership charter was established in 2017 and focuses on four equal leadership qualities and practices—reinforcing our core purpose and focus, committing to diversity and inclusion, prioritising people and culture, and leading on behalf of the whole Organisation. This leadership charter is at the heart of our culture and is reinforced by a program of leadership development and the modelling of positive day-to-day practices. Supporting this work, our Diversity and Inclusion Strategy, launched in 2018, will pave the way for ASIO to broaden our staffing profile and harness the diversity of our existing workforce.

Through our digital transformation we will build technology into every facet of our business. We will enhance the digital literacy of our workforce and adapt emerging technologies to build our capabilities in a digital world.



Partnerships

In protecting Australia, its people and its interests, we will continue to build and strengthen strategic relationships that facilitate and expand information sharing and collaboration with our partners in law enforcement and the intelligence community. We will also forge new relationships with non-traditional partners. As we design new technology platforms, and other systems, we will place an increased emphasis on interoperability, mutual benefit, data access and shared analytical techniques.

Part 5: risk oversight and management

ASIO's Executive Board is the primary advisory committee to support the Director-General in governance of the Organisation. The board provides oversight of our risk management policies, including the identification and treatment of key strategic organisational risks. The board determines whether our overall level of risk is acceptable and considers whether our risk management structures, systems and processes remain effective and support achievement of our purpose.

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 and the Executive Board on the design, operation and performance of ASIO's internal governance, risk and control framework, performance reporting, and compliance with its internal and external accountabilities and responsibilities. The ARC has four external members including an external chair.

The 2017 report *A digital transformation of the Australian Security Intelligence Organisation* recommended that ASIO develop and implement a new principles-based risk management framework. Our new risk management framework will be finalised in 2018 and will guide our approach to risk management, across all of our operational, enabling and corporate areas.

- The key activity tables in **Part 3** of this plan describe a number of high-level enduring risks to performance and the strategies we will implement to mitigate these risks.

