



Australian Government
Australian Signals Directorate

ASD

CORPORATE PLAN 2022-23



© Commonwealth of Australia 2022

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: Defence switchboard, 1300 DEFENCE (1300 333 362)

Email
asd.assist@defence.gov.au

Post
PO Box 5076, Kingston ACT 2604

Table of Contents

Foreword Deputy Prime Minister and Minister for Defence 5

Director-General’s introduction..... 7

ASD’s purpose..... 8

Our organisation..... 11

Australian Signals Directorate Strategic Plan 2022–23 to 2025–26..... 12

ASD’s operating context 14

 Environment 14

 Global shifts 14

 Technological change..... 14

 Public trust 15

 Fiscal environment 15

 Capability 16

 People and culture..... 16

 Tradecraft..... 16

 Technology 16

 Governance..... 17

 Leadership and influence 17

 Diversity and inclusion 17

 Cooperation and partnerships 18

 Risk oversight and management 20

Performance..... 21

 ASD’s performance framework 22

 ASD’s performance measures 24

 Performance Measure 1..... 24

 Performance Measure 2..... 25

 Performance Measure 3..... 26

 Performance Measure 4 27

 Performance Measure 5..... 28

 Performance Measure 6 28

 Performance Measure 7..... 29

Foreword

Deputy Prime Minister and Minister for Defence

The Australian Government is committed to keeping our nation safe and protecting our way of life.

Throughout its 75 year history, the Australian Signals Directorate (ASD) has defended Australia from global threats and advanced our national interests. It remains at the frontline of defending our nation and keeping Australia safe and secure.

As our strategic environment becomes more complex and less predictable, the work performed by ASD is more important than ever.

This Corporate Plan outlines how ASD will respond to these challenges over the next four years, including through increased investment in ASD's cyber and intelligence capabilities. This investment, known as the REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers) package, recognises the critical role ASD plays in our national security.



The Hon Richard Marles MP
Deputy Prime Minister and Minister for Defence

Director-General's introduction

I, as the accountable authority of the Australian Signals Directorate (ASD), present the 2022–23 ASD Corporate Plan, which covers the period 2022–23 to 2025–26, as required under paragraph 35(1)(b) of the Public Governance, Performance and Accountability Act 2013.

ASD's purpose is to defend Australia from global threats and advance our national interest. For 75 years, ASD's core functions to achieve this purpose have been added to, but the fundamentals have not changed. ASD's highest priority will always be the protection of Australian lives, whether that is through supporting Australia's warfighters or detecting and, in some cases, disrupting malicious threats against Australian interests.

The environment in which ASD operates is becoming increasingly challenging. Today, our region is far more complex and far less predictable than at any time since the Second World War. To meet these changes in the strategic environment, ASD must continue to evolve its capabilities. We must be able to handle the increasing complexity and volume of data, respond to new developments in technology, provide our people with the best possible tools to achieve our purpose, and be resilient to the environment. The REDSPICE package is designed to respond to these challenges.

My vision for ASD is that we are a world class intelligence, covert effects and cyber security agency, enabled by talented dedicated people, leading-edge capabilities, strong partnerships, and the trust of the Australian public – and we will continue strengthening accountability, transparency and governance of our activities to further build this trust.

This Corporate Plan outlines the steps we will take to achieve this vision in 2022–23 and beyond. ASD will evaluate and report on its performance against its purpose and key activities in the 2022–23 Annual Report.



Rachel Noble PSM
Director-General
Australian Signals Directorate

On 31 March 2022 and 1 April 2022, the National Carillon at Lake Burley Griffin in Canberra was illuminated with the Australian Signals Directorate's colours to mark ASD's 75th anniversary. For two special nights, the 50-metre tower was lit in blue, reflecting brightly on Lake Burley Griffin and lighting up the night sky. It was the first of many events celebrating 75 years of ASD's rich history and unique contribution to protecting Australia, yesterday, today and tomorrow.



ASD's purpose

The Australian Signals Directorate (ASD) defends Australia from global threats and advances the national interest by providing foreign signals intelligence, cyber security and offensive cyber operations, as directed by the Government.

ASD's purpose is achieved through the delivery of four key activities, as described in the *Defence Portfolio Budget Statements 2022–23*:

- providing foreign signals intelligence
- providing cyber security services
- conducting offensive cyber operations
- sustaining and securing future capabilities.

ASD is a statutory agency within the Defence portfolio, reporting directly to the Minister for Defence. It operates under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). All of ASD's activities are subject to oversight from the Inspector-General of Intelligence and Security (IGIS). The Parliamentary Joint Committee on Intelligence and Security (PJCS) provides further oversight of ASD's administration, expenditure and enabling legislation. It also considers other matters within its scope that are referred by the Australian Senate, House of Representatives, or a minister of the Australian Government.

ASD operates under the *Intelligence Services Act 2001* (the ISA), which specifies that the organisation's functions are to:

- collect foreign signals intelligence
- communicate foreign signals intelligence
- prevent and disrupt offshore cyber-enabled crime
- provide cyber security advice and assistance to Australian governments, businesses and individuals
- support military operations
- protect the specialised tools ASD uses to fulfil its functions
- cooperate with, and assist, the national security community's performance of its functions.

To achieve its purpose, ASD needs to keep pace with the latest technology trends and invest in cutting-edge capabilities to gain asymmetric advantage. ASD's activities are enabled by innovative techniques, including specialist tools to probe large volumes of data

to detect threats. ASD's mastery of technology also underpins the formulation of sound advice to protect Australia from sophisticated threats.

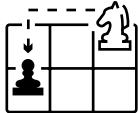
Partnerships are critical to the organisation's success. ASD works closely with the Australian national security community, overseas intelligence and cyber security partners, academia, and industry. This level of collaboration is essential to comprehensively understand the threat environment and to stay at the cutting edge of technology.

ASD's success is founded in the ingenuity of its workforce. The organisation seeks to recruit and develop a curious and imaginative workforce which is not deterred by difficult challenges. Recruiting the requisite specialist technological expertise has become increasingly challenging, given the high demand for staff with these skillsets.

This combination of a uniquely skilled workforce, empowered by innovative technology, enabled by responsible financial management, and leveraging partner capabilities, positions the organisation to deliver trusted intelligence, cyber security expertise and offensive cyber operations for Australia's national interest.

ASD's five strategic objectives

Deliver Strategic Advantage



ASD **delivers strategic advantage** for Australia by providing foreign signals intelligence that protects and advances Australia's national interest. Foreign intelligence collection activities are guided by strategic priorities set by Government.

Lead Cyber Security



ASD is the Australian Government's **leading cyber security agency**, and aims to make Australia the most secure place to connect online and to foster national cyber security resilience. ASD's Australian Cyber Security Centre (ACSC) monitors cyber threats targeting Australian interests, and provides advice and information, including through an international network of Computer Emergency Response Teams (CERTs) to help protect Australians. When serious cyber incidents occur, ASD leads the Australian Government response to help mitigate the threat and strengthen defences.

Support Military Operations



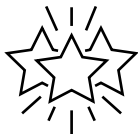
ASD has a long history of **supporting Australian military operations**, with the organisation's heritage dating back to the Second World War. Today, ASD supports Australian Defence Force (ADF) operations around the globe, including by providing intelligence and offensive cyber capabilities to enable the warfighter and protect ADF personnel and assets. ASD also draws on its deep technical expertise to help the ADF stay ahead of technology advancements in the region, including the introduction of 5th generation weapons and cyber-warfare capabilities.

Counter Cyber-Enabled Threats



ASD capabilities play an important role in **countering cyber-enabled threats**. The organisation protects Australia and Australians by preventing and disrupting offshore cyber-enabled crime, including the activities of organised criminal groups using malware to target Australians, and terrorists who use the internet to plan and incite attacks against Australian interests.

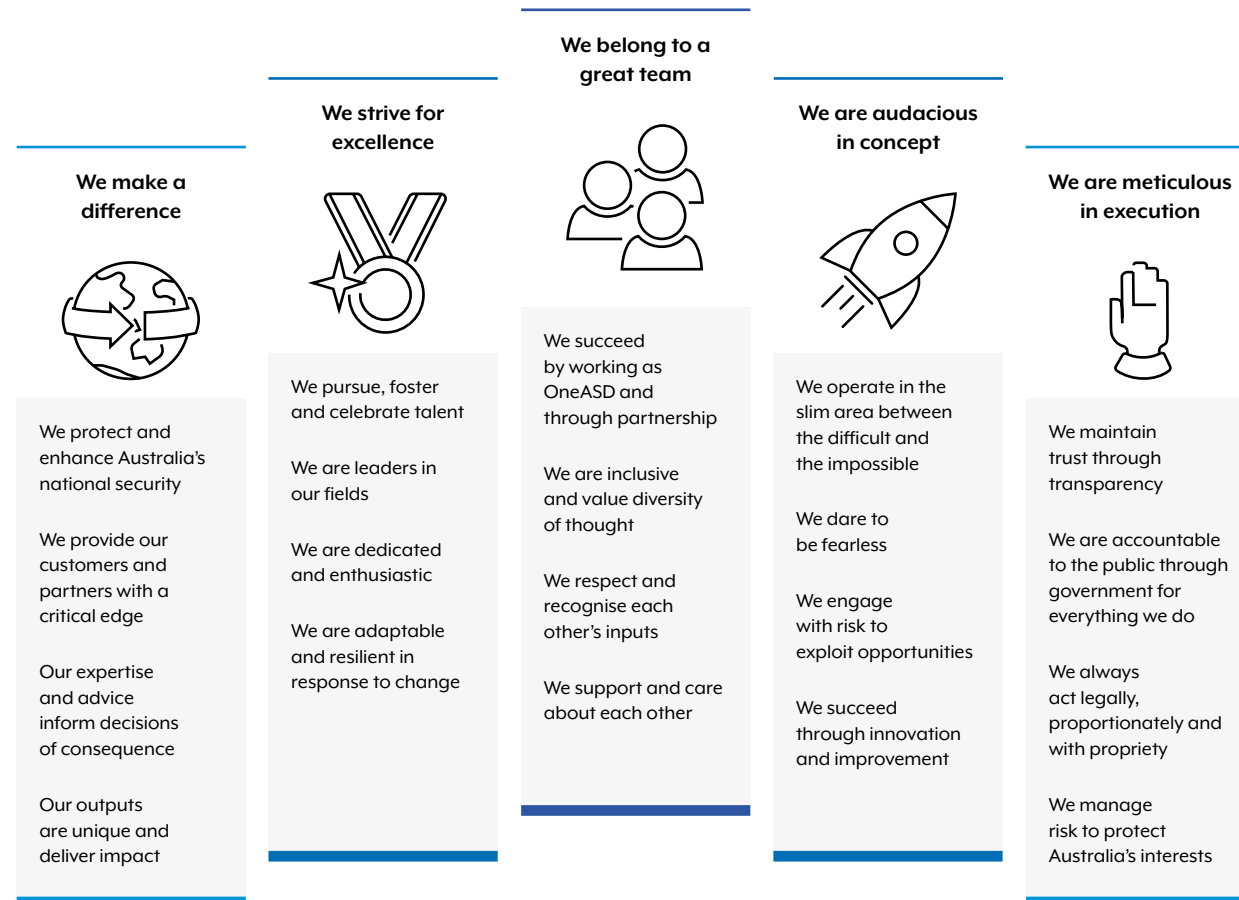
Provide Trusted Advice and Expertise



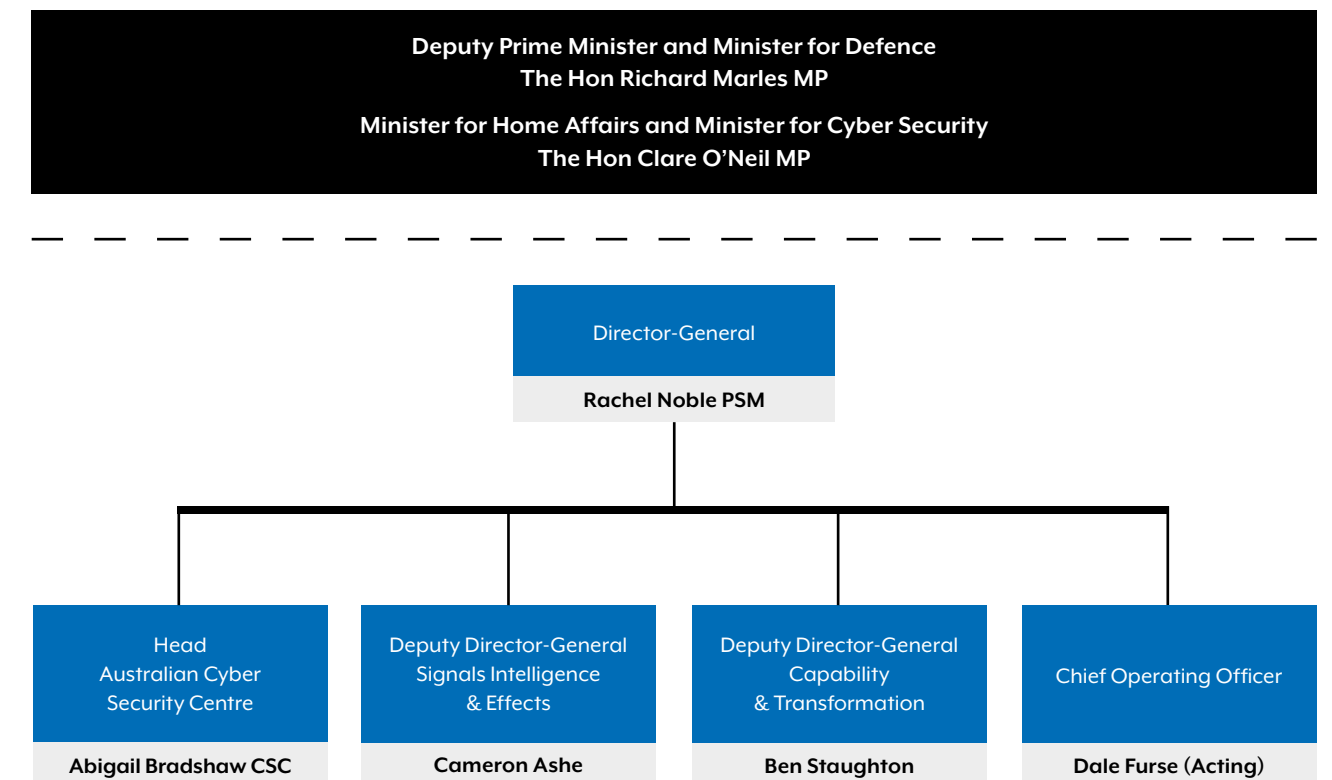
ASD provides **trusted advice and expertise** to government, business and the community. ASD draws on its deep technical understanding of communications technology to help the Australian Government and the public understand the nature of the cyber threat environment, how they might be vulnerable and what they can do to protect themselves.

OUR VALUES

Reveal their secrets. Protect our own.



Our organisation



Australian Signals Directorate Strategic Plan 2022–23 to 2025–26

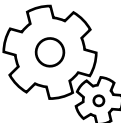
Our Purpose

Defend Australia from global threats and advance our national interests through the provision of foreign signals intelligence, cyber security and offensive cyber operations, as directed by Government.

Context & External Drivers



Global Shifts



Technological Change



Public Trust



Partnerships



Fiscal Environment

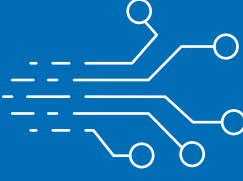


Vision

We are a world-class intelligence, covert effects and cyber security agency, enabled by talented dedicated people, leading-edge capabilities, strong partnerships, and the trust of the Australian public. Our role as both ‘poacher’ and ‘gamekeeper’ uniquely positions us to provide trusted advice and conduct intelligence operations.



We provide unique capabilities and access that inform and make a difference. We excel in the collection and exploitation of data.



We build world-class, innovative offensive cyber capabilities that deliver real-world impact.



We make Australia the most secure place to connect online.



Strategic Objectives

Deliver Strategic Advantage

Generate intelligence and operational effects to protect and advance Australia’s national interests

Lead Cyber Security

Make Australia the most secure place to connect to the online world. Foster national cyber security resilience

Support Military Operations

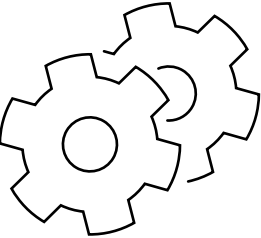
Enable the warfighter. Protect Defence personnel and assets

Counter Cyber-Enabled Threats

Protect Australia and Australians by countering cyber-enabled crime and disrupting terrorists’ use of the internet

Provide Trusted Advice and Expertise

Deliver timely, trusted and quality advice to Government, law enforcement, business and the community



Enabling Capabilities

People & Culture

Our success is based on the ingenuity and diversity of our team. We have an inclusive culture that values and rewards teamwork. We attract and retain the best talent.

Technology

We use technology in innovative and creative ways to gain asymmetric advantage. We master technology to identify and disrupt threats, and protect Australian interests.

Partnerships

We bring together our expertise and capabilities with those of our partners for mutual benefit. Respectful relationships and collaboration enable our success.

Tradecraft

We give our staff the skills to solve challenging problems, and operate in the slim area between the difficult and the impossible.

Governance & Risk

We act professionally, legally and ethically. We manage risk and are fully accountable for our actions. We are fiscally responsible, and we promote a culture that values strong compliance and security practices.

Leadership & Influence

The leadership skills of our people underpin everything we do. And our mastery of technology underpins our trusted advice to the Government and public.

Our Values

We make a difference

We strive for excellence

We belong to a great team

We are audacious in concept

We are meticulous in execution

12

13

ASD’s operating context

ASD’s ability to deliver the outcomes described in its corporate plan is influenced by changes in its operating environment. These changes are key to ASD’s efforts to evolve its business, ensuring it is well-positioned to continue to help keep Australia safe.

Environment



GLOBAL SHIFTS

Australia’s security and prosperity rely on a secure, stable, prosperous, rules-based region. As communicated in the *Defence Strategic Update 2020*, our region is in the midst of the most consequential strategic realignment since the Second World War. The Indo-Pacific is at the centre of a greater strategic competition, making the region more contested and apprehensive: military modernisation has accelerated faster than expected, major power competition has intensified, and the conduct of ‘grey zone’ activities has expanded.

ASD’s capabilities provide the Australian Government with intelligence, covert effects and cyber security expertise that deliver strategic advantage, policy and advice that protects national security and sovereignty, and practical support that informs law enforcement and military operations. Across the life of this corporate plan, ASD will continue to invest in developing its workforce and technology to ensure it responds flexibly to the changing priorities of the Australian Government.



TECHNOLOGICAL CHANGE

Technological advances provide great benefit to society, but these advances also introduce risks.

ASD’s mastery of technology enables it to protect Australia from global threats. But technology is evolving rapidly. State and non-state actors can access increasingly sophisticated communication technologies and the tools used to exploit them.

ASD has a dual role as a trusted advisor in assisting the Australian Government to navigate major technological change, and to exploit technology to deliver foreign signals intelligence, cyber security and offensive cyber operations in support of Australian Government priorities.

ASD has always evolved its capabilities in response to technological change. In the years covered by this corporate plan, the challenge of maintaining mastery of technology will become more complex and demanding. To meet this challenge, ASD will enhance science, technology, engineering and mathematics (STEM) skills in its workforce and invest in new and emerging technologies, including the delivery of the next-generation data science and artificial intelligence.



PUBLIC TRUST

As an intelligence agency, ASD has been entrusted with sensitive powers. ASD takes this responsibility very seriously.

ASD’s functions are set out in the ISA, along with the limitations on these functions. Under this legislation, ASD is accountable for its actions to the Australian Government, the Minister for Defence, and the IGIS – which has the powers of a standing Royal Commission – to provide independent assurance that ASD acts legally and ethically.

ASD recognises the importance of maintaining the trust of the Australian Government and the Australian public.

While, for security reasons, ASD may not be able to share the details of its operations, ASD seeks to increase the information it shares with Australians about its functions. ASD is committed to assisting Australians in understanding the principles on which ASD makes decisions, the way it protects the privacy of Australians, and its strong culture of operating within the spirit and letter of the law.



FISCAL ENVIRONMENT

The Australian Government has made significant investments in building ASD’s foreign signals intelligence, cyber security and offensive cyber capabilities. This includes a \$9.9 billion investment in cyber and intelligence capabilities over the next decade through the REDSPICE package.

ASD is continuing to refine and enhance its governance and accountability frameworks, including enterprise performance management and fit-for-purpose financial management systems, to ensure it is operating efficiently, sustainably and responsibly within its forward budget. ASD will build on its strong foundation of governance, and will establish a dedicated external advisory board to support the efficient and effective delivery of REDSPICE capabilities.

Capability

ASD’s capabilities enable it to deliver on its purpose and strategic objectives. For the duration of this corporate plan, ASD will place special emphasis on building and enhancing the capabilities needed to meet the challenges of the evolving strategic environment, including changes in technology and data analysis. It will invest in improving leadership skills and building a culture that leverages the strength of a diverse and capable workforce. It will build and foster partnerships to deliver value in this complex operating environment.



People and culture

ASD’s people are its greatest resource. The skills and experience of its people are in high demand across private industry and government. To ensure its success, ASD must accelerate its efforts to attract, develop and retain a diverse and highly skilled workforce. Over the life of this corporate plan, ASD will significantly expand its workforce, creating new jobs at locations across Australia.



Tradecraft

ASD’s foreign signals intelligence, cyber security and offensive cyber operations missions require a highly skilled workforce, equipped with the right skills to be effective and successful at delivering its missions. The pace of technological change and the evolving threat landscape increase ASD’s opportunities to develop new tradecraft, but also increase the challenge of keeping ahead. ASD needs to ensure that its analysts are equipped with the right skills and can deploy modern tradecraft against ASD’s toughest analytical problems.



Technology

Technology is at the heart of ASD’s capability. Mastering and adapting to technological change is crucial to enabling ASD’s ongoing success in delivering foreign signals intelligence, cyber security, and offensive cyber operations.



Governance

ASD’s status as a statutory agency has given it the autonomy to build enterprise governance and risk frameworks that are tailored to the unique nature of ASD’s work. As part of this work, ASD has established robust compliance and oversight processes, which provide assurance that ASD acts within the spirit and letter of the laws that enable us.



Leadership and influence

The leadership skills of ASD’s people – at all levels of the organisation – are vital to its success. ASD’s leaders are at the forefront of delivering strategic initiatives, and supporting and developing the workforce.



Diversity and inclusion

ASD’s workforce operates in the slim area between the difficult and the impossible. Solving the toughest problems in foreign signals intelligence, cyber security and offensive cyber operations requires teams of clever, curious people with diverse and complementary skills. ASD’s strength, resilience, and creativity is derived from the different ages, backgrounds, genders, cultures, neurodiversity, physical abilities, religions and sexualities of its staff. ASD is committed to providing a respectful and inclusive workplace.

Cooperation and partnerships

In a complex and evolving world, ASD cannot operate effectively alone. Strong partnerships underpin ASD’s ability to understand global threats, collect foreign signals intelligence, formulate and implement cyber security advice, and conduct offensive cyber operations in support of the Australian Government.

ASD has a long history of working effectively with its partners in the National Intelligence Community (NIC), Australian federal, state, and local government entities, the ADF, academia, and industry. ASD collaborates across the private and public sector, providing advice and assistance to prevent and combat threats and minimise harm to Australians.

ASD has long-standing, robust and meaningful ties with its Five-Eyes counterparts in the United States of America, the United Kingdom, Canada, and New Zealand, as well as other international partnerships including through the international network of CERTs.

In the period covered by this corporate plan, ASD will strengthen partnerships with its counterpart agencies, state, territory and federal government agencies, industry, academia, and think-tanks to meet the Australian Government’s strategic objectives and operational needs. ASD will also continue to strengthen partnerships with all levels of government, critical infrastructure operators and Australian businesses to boost Australia’s whole-of-economy cyber defence capabilities. An expanded national and international footprint will enable ASD to integrate more closely with its partners and improve the resilience of our key activities.



Risk oversight and management

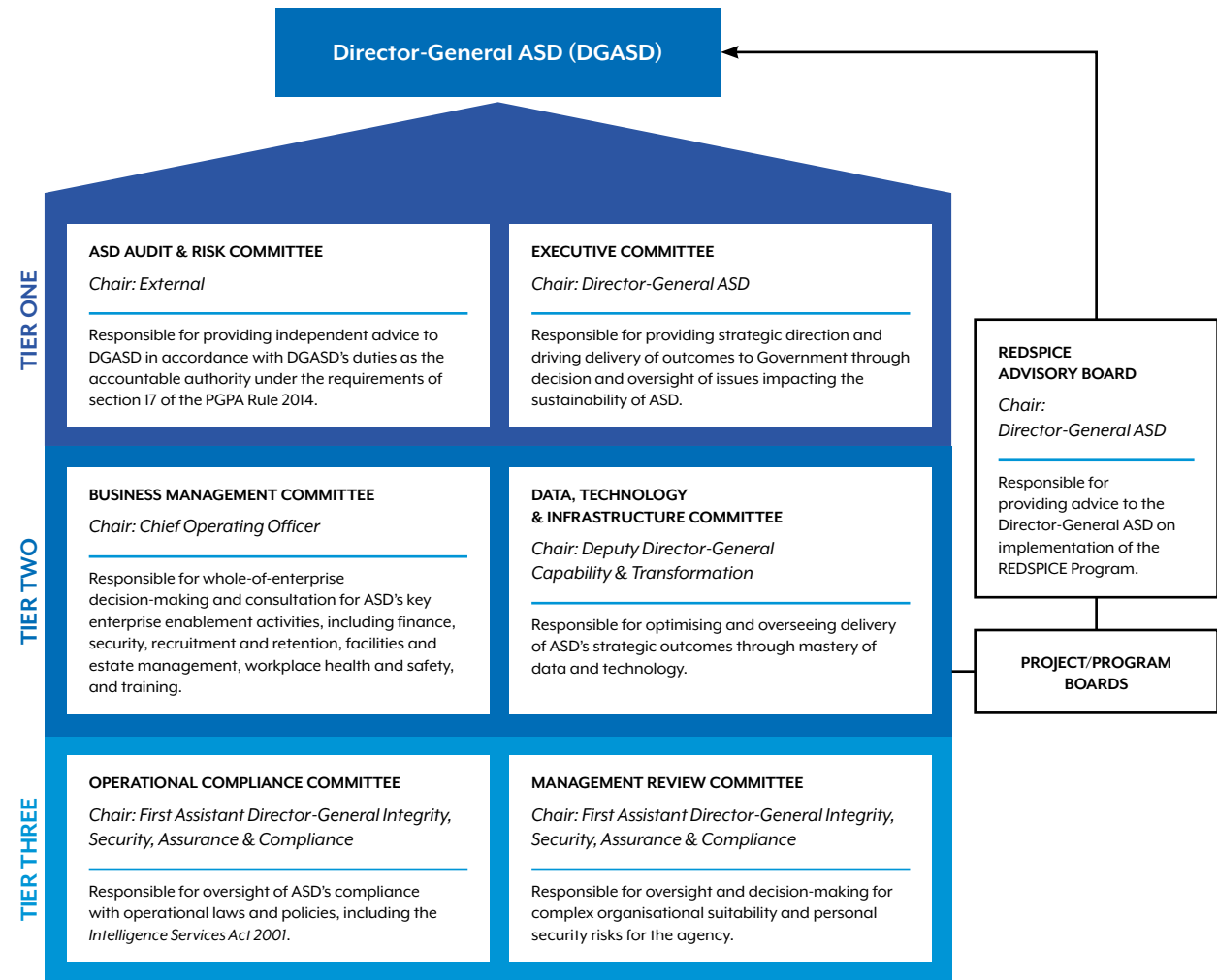
Executive committee structure

ASD’s Executive Committee is the primary advisory committee to support the Director-General in the oversight of all ASD functions. The committee defines operational and corporate risk tolerances, and oversees effective risk management across the agency. The Director-General is supported in these functions by ASD’s governance framework and committees.

The ASD Audit and Risk Committee (ASDARC) was established in 2018 to comply with section 45 of the PGPA Act. The ASDARC provides independent assurance of ASD’s risk management framework, internal governance, and performance. It provides independent advice to the Director-General with respect to financial reporting, ASD’s system of oversight and management, ASD’s system of internal control, and internal and external audit reports.

An external REDSPICE Advisory Board has been established to provide the Director-General ASD with independent advice on delivery of the REDSPICE Program.

ASD continues to embed risk management principles to support timely decision-making and reporting, prioritisation of resources, increased compliance and efficiency, and continual improvement in operations. ASD has an endorsed Enterprise Risk Management Policy, which outlines our approach to managing risks and how this supports our strategic objectives. The policy provides a list of responsibilities for all staff, including managers, risk owners and control owners. It will be reviewed annually, or as directed by Director-General ASD.



Performance

ASD’s purpose is to defend Australia from global threats and advance the national interest through providing foreign signals intelligence, cyber security support and conducting offensive cyber operations, as directed by the Australian Government. While ASD’s purpose will not change significantly over the duration of this corporate plan, the way in which ASD meets the needs of Australians and the Australian Government will evolve in response to shifts in its operating context and changes in the global threat environment.

As outlined in the *Portfolio Budget Statements 2022–23*, ASD has established seven performance measures to support the evaluation of ASD’s performance against its key activities and purpose.

For the duration of this corporate plan, ASD will assess and measure its performance through a mix of qualitative and quantitative methods. The performance measures, targets and evaluation methodology are detailed in the following tables. Performance targets carry equal weight and where a performance criterion has one or more targets, success will be measured by the proportion of targets achieved.

Qualitative performance measures will be assessed based on the impact of the product or service provided by ASD to its customers. Where ASD has indicated that its target is high impact, this means that the output will be delivered in a timely and relevant manner, will provide or enable exercisable options, and will directly inform and shape decision-making. ASD will use case studies to demonstrate high impact and will select activities reflecting ASD’s highest priority missions and/or a shift in operational resourcing.

Due to the nature of ASD’s work, some aspects of ASD’s performance will continue to be reported through classified channels.

ASD’s performance framework

PURPOSE						
The Australian Signals Directorate defends Australia from global threats and advances the national interest through the provision of foreign signals intelligence, cyber security and offensive cyber operations, as directed by Government.						
STRATEGIC OBJECTIVES						
Deliver Strategic Advantage, Lead Cyber Security, Support Military Operations, Counter Cyber-enabled Threats, Provide Trusted and Expert Advice.						
KEY ACTIVITIES						
Provide Foreign Signals Intelligence		Provide Cyber Security Services		Conduct Offensive Cyber Operations		Sustain & Secure Future Capabilities
Performance Measures						
1. ASD's foreign signals intelligence meets Government's expectations to deliver strategic advantage and enables National Intelligence Community operations.	2. ASD's foreign signals intelligence products and technical expertise provide effective support for military operations and activities.	3. ASD provides high quality, impactful cyber security services to government, critical infrastructure and services, business, families and individuals.	4. ASD delivers partnerships, programs and technical capability that strengthen national cyber security or resilience.	5. ASD's offensive cyber operations provide effective and timely support for military operations and activities.	6. ASD's offensive cyber activities meet whole-of-government security requirements to counter offshore cyber threats.	7. ASD's corporate services, and technology platforms and products ¹ support the achievement of mission ² outcomes.
Performance Metrics						
1.1. Government expectations to deliver strategic advantage are met.	2.1. ASD's foreign signals intelligence support the ADF's military operations and activities, technological advantage and capability development.	3.1. ASD's cyber security advice and assistance supports stakeholders to improve or maintain their cyber security posture.	4.1. Cyber security information and expertise exchanges with partners help prevent, detect or remediate cyber threats to Australia.	5.1. Offensive cyber capabilities provide effective and timely support for ADF military operations and activities.	6.1. Offensive cyber operations that counter offshore cyber threats meet whole-of-government requirements.	7.1. ICT infrastructure and services support mission operations and corporate services.
1.2. National Intelligence Community operational requirements are met.		3.2. Systems to support assistance and technical advice are available for use by ASD and relevant stakeholders.	4.2. ASD supports emerging cyber security research that may help prevent, detect or remediate cyber threats to Australia.			7.2. ASD's workforce meets mission requirements.
		3.3. ASD's Top Secret network accreditation and key management services support stakeholders' requirements.				

1 ‘Technology platforms and products’ refers to ICT hardware and software, for both classified and unclassified networks, that is used or supported by ASD.
2 ‘Mission’ refers to the three Key Activities to provide foreign signals intelligence, provide cyber security service, and conduct offensive cyber operations.

ASD’s performance measures

The performance information outlined in this corporate plan and the *Portfolio Budget Statements 2022–23* will be used as the basis for ASD’s 2022–23 annual performance statements. The performance measures have been developed to meet the guidance in section 16EA of the *Public Governance, Performance and Accountability Rule 2014*.

KEY ACTIVITY: PROVIDE FOREIGN SIGNALS INTELLIGENCE	
Performance Measure 1	
ASD’s foreign signals intelligence meets Government’s expectations to deliver strategic advantage and enables National intelligence Community (NIC) operations.	
Metrics	How success will be measured (targets)
1.1 Government expectations to deliver strategic advantage are met.	Government and NIC stakeholders confirm that ASD products have high impact.
1.2 NIC operational requirements are met.	NIC and Defence stakeholders confirm that ASD products have high impact.
Data sources and methodology	
- NIC evaluations of ASD’s intelligence products, technical expertise and advice. - Analysis of feedback from Government, Defence and NIC agencies. - Analysis of feedback on request for information answered by ASD to support or inform NIC operations.	
Timeline	2022–23 to 2025–26

Performance Measure 2	
ASD’s foreign signals intelligence products and technical expertise provide effective support for military operations and activities.	
Metrics	How success will be measured (targets)
2.1 ASD’s foreign signals intelligence supports the ADF’s military operations and activities, technological advantage and capability development.	ADF/Defence stakeholders confirm ASD support had a high impact.
Data sources and methodology	
- Analysis of feedback on the efficacy, timeliness and value of ASD’s intelligence products and expertise. - Analysis of feedback on ASD’s support for ADF capability advantage.	
Timeline	2022–23 to 2025–26

KEY ACTIVITY: PROVIDE CYBER SECURITY SERVICES

Performance Measure 3

ASD provides high quality, impactful cyber security services to government, critical infrastructure and services, business, families and individuals.

Metrics	How success will be measured (targets)
3.1 ASD's cyber security advice and assistance supports stakeholders to improve or maintain their cyber security posture.	Information Security Manual (ISM) and Essential Eight (E8) are updated at least annually.
	Number of Infosec Registered Assessors Program (IRAP) assessors remains constant or increases.
	Demonstrated impact.
3.2 Systems to support assistance and technical advice are available for use by ASD and relevant stakeholders.	Availability of support assistance and technical advice remains at or above 99%.
3.3 ASD's Top Secret network accreditation and key management services support stakeholders' requirements.	All requests are resolved within timeframes agreed with the stakeholder.
	Availability remains at or above 99%.

Data sources and methodology

- Number of times the ISM and E8 are updated.
- Qualitative analysis of impact of advice and technical support provided to partners, industry and Government.
- Number of endorsed IRAP assessors listed on *cyber.gov.au*.
- Percentage of time *cyber.gov.au*, the ACSC Partnerships Portal, 24/7 Call Centre support, and ReportCyber are available.
- Percentage of requests for Top Secret accreditation/certification resolved in a timely manner.
- Percentage of time cryptographic key infrastructure is available.

Timeline2022–23 to 2025–26

Performance Measure 4

ASD delivers partnerships, programs and technical capability that strengthen national cyber security or resilience.

Metrics	How success will be measured (targets)
4.1 Cyber security information and expertise exchanges with partners help prevent, detect or remediate cyber threats to Australia.	Number of ACSC Partners increases.
	Demonstrated impact.
4.2 ASD supports emerging cyber security research that may help prevent, detect or remediate cyber threats to Australia.	Demonstrated impact.

Data sources and methodology

- Membership numbers of the ACSC Partnership Program.
- Qualitative analysis of impact of support to domestic partners, including Government and industry.
- Qualitative analysis of impact of support to international partners.
- Qualitative assessment of impact of engagement to support cyber security research.

Timeline2022–23 to 2025–26

KEY ACTIVITY: CONDUCT OFFENSIVE CYBER OPERATIONS	
Performance Measure 5	
ASD's offensive cyber operations provide effective and timely support for military operations and activities.	
Metrics	How success will be measured (targets)
5.1 Offensive cyber capabilities provide effective and timely support for ADF military operations and activities.	ADF/Defence stakeholders confirm ASD support had a high impact.
Data sources and methodology	
Analysis of ADF/Defence feedback on efficacy, timeliness and value of ASD's offensive cyber support to military operations and activities.	
Timeline	2022–23 to 2025–26

Performance Measure 6	
ASD's offensive cyber activities meet whole-of-government security requirements to counter offshore cyber threats.	
Metrics	How success will be measured (targets)
6.1 Offensive cyber operations that counter offshore cyber threats meet whole-of-government security requirements.	Government stakeholders confirm ASD operations had a high impact.
Data sources and methodology	
Analysis of Government feedback on the efficacy, timeliness and value of ASD's offensive cyber operations to counter offshore cyber threats.	
Timeline	2022–23 to 2025–26

KEY ACTIVITY: SUSTAIN AND SECURE FUTURE CAPABILITY	
Performance Measure 7	
ASD's corporate services and technology platforms and products support the achievement of mission outcomes.	
Metrics	How success will be measured (targets)
7.1 ICT infrastructure and services support mission operations and the delivery of corporate services.	Year-on-year improvement in ICT service.
	ICT projects delivered to implement ASD's Enterprise Technology Strategy.
7.2 ASD's workforce meets mission requirements.	24/7 support for mission critical systems. Business hours support for non-mission critical systems. Available across domestic and overseas ASD sites.
	Year-on-year improvement in the percentage of systems development within agreed interoperability standards.
7.2 ASD's workforce meets mission requirements.	Year-on-year improvement in delivery of recruitment and retention initiatives.
	Year-on-year improvement in the percentage of staff that have met mandatory training requirements.
	Year-on-year improvement in the number of staff that have attended leadership and management skills courses.
7.2 ASD's workforce meets mission requirements.	Year-on-year improvement in the number of staff that have attended tradecraft (customised) training courses.
Data sources and methodology	
- Qualitative analysis of stakeholder feedback regarding the provision of quality, responsive ICT service to meet mission and corporate requirements. - Service management statistics. - Data on ICT projects delivered on time and within budget. - Data on systems developed within agreed interoperability standards. - Qualitative analysis of ASD initiatives to attract and retain a skilled workforce. - Defence and ASD Training Systems data.	
Timeline	2022–23 to 2025–26

