



Australian Government
Australian Signals Directorate

ASD

CORPORATE PLAN 2025-26



© Commonwealth of Australia 2025

Unless otherwise noted, copyright (and other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia.



With the exception of the Commonwealth Coat of Arms, this work is licensed under a Creative Commons Attribution 4.0 International license ([CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)).

You may not reproduce or use any material presented in this publication in any way that suggests the Australian Signals Directorate (ASD) endorses you, your commentary, or any of your services or products.

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 (<https://www.pmc.gov.au/honours-and-symbols/commonwealth-coat-arms>).

Contact us

Phone

General inquiries: 1300 DEFENCE (1300 333 362)
Cyber Security Hotline: 1300 CYBER1 (1300 292 371)

Email

asd.assist@defence.gov.au

Post

Assistant Director-General Governance
Australian Signals Directorate
PO Box 5076,
Kingston ACT 2604

Acknowledgment of Country

ASD acknowledges the Traditional Owners and Custodians of Country throughout Australia, and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, the cultures and Elders past and present. We also acknowledge the contributions of our Aboriginal and Torres Strait Islander employees in support of our mission.

Table of Contents

Director-General’s introduction..... 1

ASD’s purpose..... 2

 ASD’s five strategic objectives..... 3

Our values..... 4

Our organisation..... 5

Australian Signals Directorate Strategic Plan 2025–26 to 2028–29 6

ASD’s operating context 8

 Environment 8

 Global shifts 8

 Technological change 8

 Public trust 9

 Fiscal environment 9

 Capability 10

 People and culture..... 10

 Tradecraft..... 10

 Technology 10

 Governance..... 11

 Leadership and influence 11

 Diversity and inclusion 11

 Cooperation and partnerships 12

 Risk oversight and management..... 12

Performance..... 15

 ASD’s performance framework 16

 ASD’s performance measures 18

 Performance Objective 1 18

 Performance Objective 2 19

 Performance Objective 3 20

 Performance Objective 4 21

 Performance Objective 5 22

Director-General's introduction

I, as the accountable authority of the Australian Signals Directorate (ASD), present the ASD Corporate Plan 2025–26, which covers the period 2025–26 to 2028–29, as required under section 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 interests through the provision of foreign signals intelligence, cyber security and offensive cyber operations, as directed by Government.

ASD achieves this purpose by providing critical support to the Australian Defence Force (ADF) and working with the National Intelligence Community (NIC), as well as whole-of-government and international partners, to ensure our signals intelligence and cyber capabilities are leading-edge.

As outlined in the National Defence Strategy 2024, Australia faces its most complex and challenging strategic environment since the Second World War, with entrenched and increasing competition a primary feature of Australia's security environment.

In response to this environment, ASD continues to implement the REDSPICE program, which enhances and improves the resilience of Australia's cyber, intelligence capabilities and communications.

My vision for ASD is one of continuous innovation, responsibly leveraging rapid technological change and enabled by strong partnerships and a skilled, diverse workforce dedicated to protecting our national interests. We strive to maintain trust among our stakeholders, the Government and the Australian public, through a commitment to good governance, transparency and accountability.

This corporate plan outlines the steps we will take to achieve this vision in 2025–26 and beyond. ASD will evaluate and report on its performance against its purpose and key activities in the 2025–26 Annual Report.



Abigail Bradshaw CSC
Director-General
Australian Signals Directorate

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 Government.

ASD's purpose is achieved through the delivery of three key activities, as described in the *Defence Portfolio Budget Statements 2025–26*:

- providing foreign signals intelligence
- providing cyber security services
- conducting offensive cyber operations.

Additional capability-focused performance measures have been included in this corporate plan.

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 (PJICIS) 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.

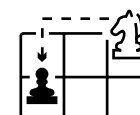
ASD's success is founded on the ingenuity of its workforce. It seeks to recruit and develop a curious and imaginative workforce that is not deterred by difficult challenges. Recruiting the requisite specialist technological expertise has become increasingly challenging, given the high demand for staff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

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

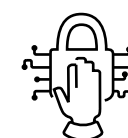
In support of delivering our purpose, ASD has five strategic objectives.

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 to help protect Australians. When serious cyber incidents occur, ASD leads the Australian Government's response to help mitigate the threat and strengthen defences.

Support Military Operations



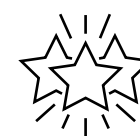
ASD has a long history of **supporting Australian military operations**, with the organisation's heritage dating back to the Second World War. Today, ASD supports Australian Defence Force (ADF) operations around the globe, including by providing intelligence and offensive cyber capabilities to enable 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.

We make a difference




We protect and enhance Australia's national security

We provide our customers and partners with a critical edge

Our expertise and advice inform decisions of consequence

Our outputs are unique and deliver impact

We strive for excellence




We pursue, foster and celebrate talent

We are leaders in our fields

We are dedicated and enthusiastic

We are adaptable and resilient in response to change

We belong to a great team



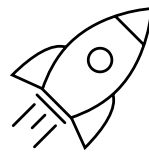
We succeed by working as OneASD and through partnership

We are inclusive and value diversity of thought

We respect and recognise each other's inputs

We support and care about each other

We are audacious in concept




We operate in the slim area between the difficult and the impossible

We dare to be fearless

We engage with risk to exploit opportunities

We succeed through innovation and improvement

We are meticulous in execution



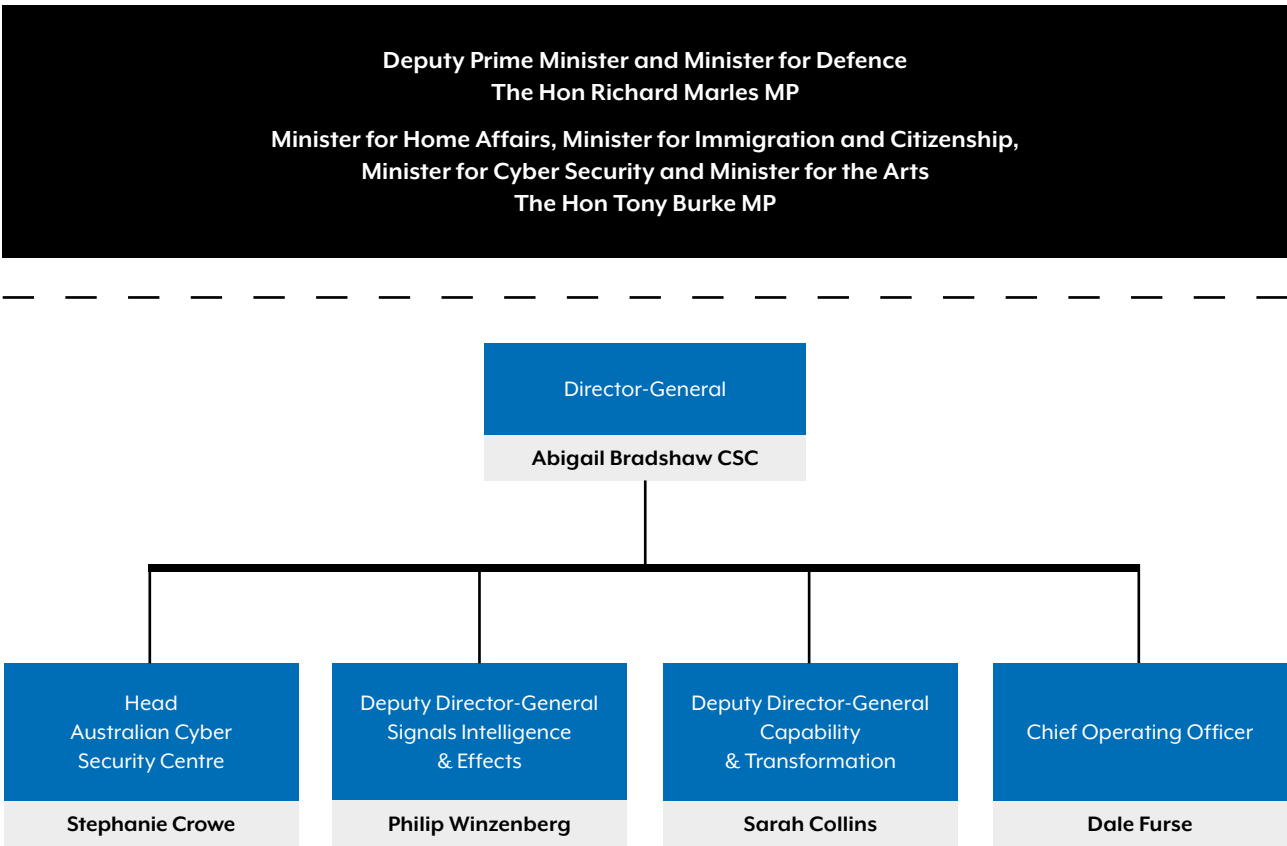
We maintain trust through transparency

We are accountable to the public through Government for everything we do

We always act legally, proportionately and with propriety

We manage risk to protect Australia's interests

Our organisation




Australian Signals Directorate Strategic Plan 2025–26 to 2028–29

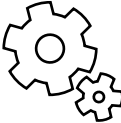
Our Purpose

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

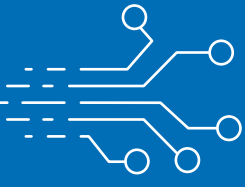


Vision


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

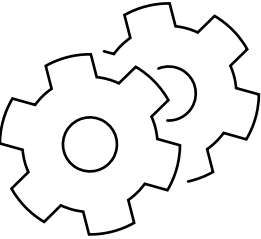
Enable the warfighter. Protect Defence personnel and assets

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

6

7

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

The 2024 National Defence Strategy acknowledges that Australia’s security and prosperity are inextricably linked. Australia’s future depends in large part upon protecting our economic connection to the world, upholding the global rules-based order, maintaining a favourable regional strategic balance and contributing to the collective security of the Indo-Pacific.

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 to the Australian Government to help it 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 – who 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 a significant investment in building ASD’s foreign signals intelligence, cyber security and offensive cyber capabilities.

The Government has prioritised REDSPICE funding in the 2024 Integrated Investment Program to enhance Australia’s cyber capabilities, intelligence, surveillance and reconnaissance and deliver resilient communications and computer network defence and disrupt options.

ASD continues 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 continue to build on its strong foundation and culture of good governance.

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 that is equipped with the right skills to be effective and successful at delivering ASD 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. ASD’s ICT infrastructure and services will continue to evolve in support of mission operations and the delivery of corporate services. This includes the delivery of enabling technical capability to the NIC and the ADF.



Governance

As a statutory agency, ASD has enterprise governance and risk frameworks that are tailored to the unique nature of the agency’s work. As part of this work, ASD operates 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 are 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 support ASD to achieve its purpose by underpinning its 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 NIC, Australian federal, state, territory 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 Computer Emergency Response Teams.

In the period covered by this corporate plan, ASD will strengthen partnerships with its international 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 its key activities.

Risk oversight and management

Risk and risk management

Risk is inherent in every aspect of ASD’s mission. Our key categories of enterprise risk are:

- Loss of licence to operate
- Operational exposure
- Intelligence failure
- Disruptive technologies and data science
- Compliance with the law
- Delivering on cyber security
- Workforce
- Morale and wellbeing
- Protective security.

Risk management is incorporated in all facets of ASD, from embedding a positive risk culture in the agency, to effective risk management practices and decision-making processes.

ASD mitigates risk by implementing a risk management program that uses risk controls as the mechanism to reduce inherent risk to within directed risk tolerance levels.

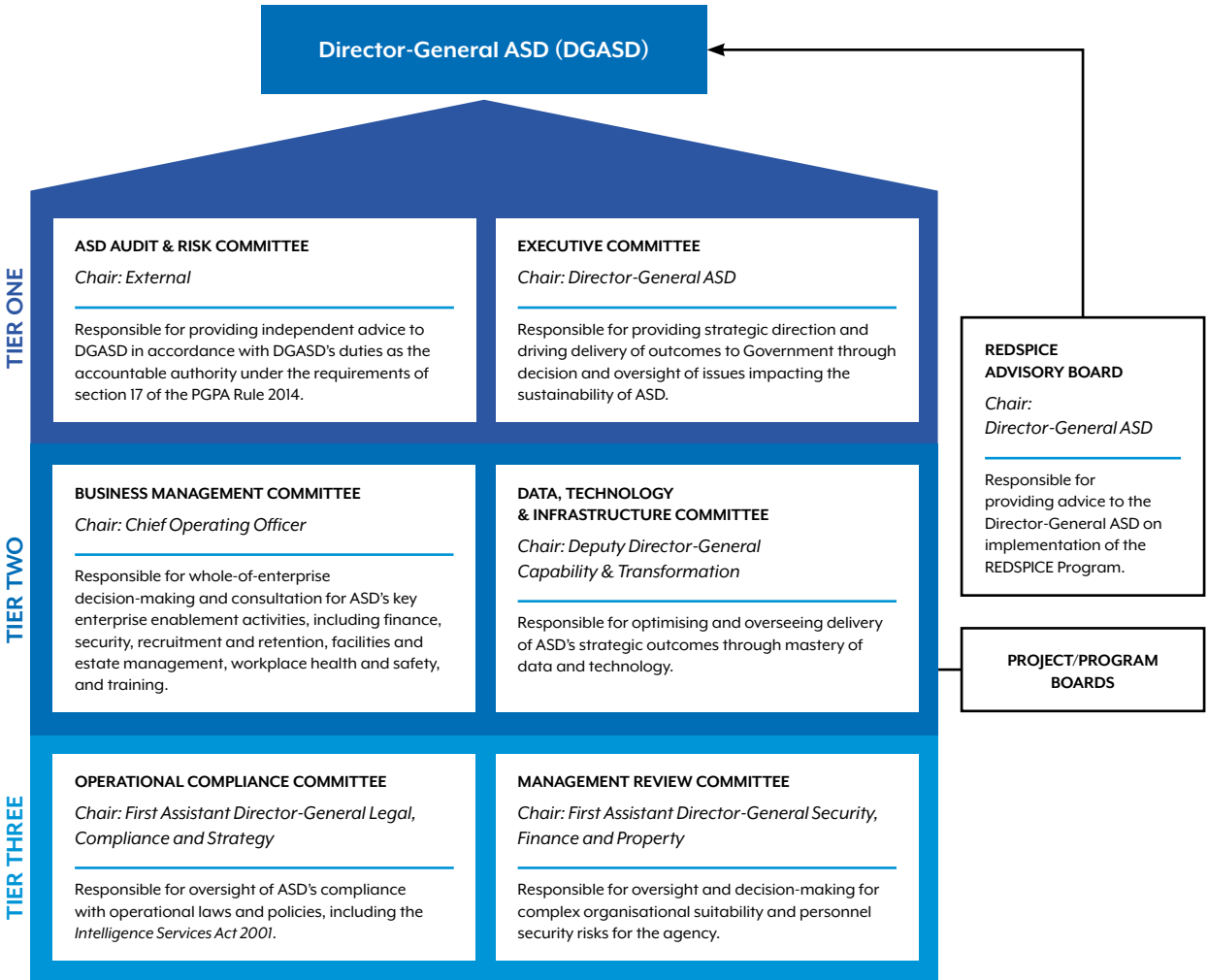
ASD’s *Risk Management Policy and Framework* defines key responsibilities, risk appetites and risk tolerances. This allows project, program, operational and specialist risks to be identified, assessed and consistently managed by individual business areas. This model is supported by a central risk function that coordinates reporting and analysis for senior decision makers.

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.

Executive Committee structure

ASD’s Executive Committee is the primary advisory committee that supports 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.

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





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 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.

ASD has reviewed its performance objectives and identified opportunities to mature and improve its performance information in line with Department of Finance guidance, as well as findings from the Australian National Audit Office's recent audits of Performance Statements in the Commonwealth. ASD has widened the performance information in this corporate plan by amending performance objectives to report the delivery of enabling technical capability.

For the duration of this corporate plan, ASD will assess and measure its performance through a mix of qualitative and quantitative assessments. 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.

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

The ASD Audit and Risk Committee (ASDARC) was established in 2018 to comply with section 45 of the PGPA Act. ASDARC 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.

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
Performance Objectives				
1. ASD's foreign signals intelligence products and enabling capabilities meet Government's expectations to deliver strategic advantage and support National Intelligence Community (NIC) operations.		3. ASD provides high-quality, impactful cyber security services to government, critical infrastructure and services, business, families and individuals.		5. ASD's offensive cyber operations provide effective and timely support for military operations and activities, and meet whole-of-government requirements for countering offshore cyber threats.
2. ASD's foreign signals intelligence products and technical expertise provide effective support for military operations and activities.		4. ASD delivers partnerships, programs and technical capability that strengthen national cyber security or resilience.		
Performance Measures				
1.1. Government expectations to deliver strategic advantage are met.		3.1. ASD's cyber security advice and assistance supports stakeholders to improve or maintain their cyber security posture.		5.1. Offensive cyber capabilities provide effective and timely support for ADF military operations and activities.
2.1. ASD's foreign signals intelligence and enabling capabilities support the ADF's military operations and activities, technological advantage and capabilities.		4.1. Cyber security information and expertise exchanges with partners help prevent, detect or remediate cyber threats to Australia.		
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.		5.2 Offensive cyber operations that counter offshore cyber threats meet whole-of-government requirements.
		3.3. ASD's Top Secret network assessment and authorisation activities and key management services support stakeholders' requirements.		

ASD’s performance measures

The performance information outlined in this corporate plan and the *Defence Portfolio Budget Statements 2025–26* will be used as the basis for ASD’s 2025–26 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, and have been broadened in this reporting period to report the delivery of technical capability.

KEY ACTIVITY: PROVIDE FOREIGN SIGNALS INTELLIGENCE	
Performance Objective 1	
ASD’s foreign signals intelligence products and enabling capabilities meet Government’s expectations to deliver strategic advantage and support National Intelligence Community (NIC) operations.	
Measures	How success will be measured (targets)
1.1 Government expectations to deliver strategic advantage are met.	Government and NIC stakeholders confirm that ASD products had a high impact.
1.2 NIC operational requirements are met.	NIC and Defence stakeholders confirm that ASD’s products and enabling capabilities had a high impact.
Data sources and methodology	
<ul style="list-style-type: none">NIC evaluations of ASD’s intelligence products, enabling capabilities, technical expertise and advice.Analysis of feedback from Government, Defence and NIC agencies.Analysis of customer feedback received by ASD.	
Timeline	2025–26 to 2028–29
This Performance Objective has been amended to measure the performance of ASD in delivering technical capability to support Government and the NIC.	

Performance Objective 2	
ASD’s foreign signals intelligence products and technical expertise provide effective support for military operations and activities.	
Measures	How success will be measured (targets)
2.1 ASD’s foreign signals intelligence and enabling capabilities support the ADF’s military operations and activities, technological advantage and capabilities.	ADF/Defence stakeholders confirm ASD support had a high impact.
Data sources and methodology	
<ul style="list-style-type: none">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 capabilities.	
Timeline	2025–26 to 2028–29
This Performance Objective has been amended to measure the performance of ASD in delivering technical capability to support the ADF.	

KEY ACTIVITY: PROVIDE CYBER SECURITY SERVICES	
Performance Objective 3	
ASD provides high quality, impactful cyber security services to Government, critical infrastructure and services, business, families and individuals.	
Measures	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 assessment and authorisation activities, and key management services support stakeholders' requirements.	All requests are resolved within the timeframes agreed with the stakeholder.
	Availability remains at or above 99%.
Data sources and methodology	
<ul style="list-style-type: none">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 requests for Top Secret assessments and authorisations resolved in a timely manner.Percentage of times customers have access to cryptographic keying material.Number of times cyber.gov.au is accessed and products on cyber.gov.au are downloaded.	
Timeline	2025–26 to 2028–29

Performance Objective 4	
ASD delivers partnerships, programs and technical capability that strengthen national cyber security or resilience.	
Measures	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	
<ul style="list-style-type: none">Membership numbers of ASD's Cyber Security 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.	
Timeline	2025–26 to 2028–29

KEY ACTIVITY: CONDUCT OFFENSIVE CYBER OPERATIONS

Performance Objective 5

ASD’s offensive cyber operations provide effective and timely support for military operations and activities, and meet whole-of-government requirements for countering offshore cyber threats.

Measures	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.
5.2 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 ADF/Defence feedback on efficacy, timeliness and value of ASD’s offensive cyber support to military operations and activities.
- Analysis of Government feedback on the efficacy, timeliness and value of ASD’s offensive cyber operations to counter offshore cyber threats.
- Analysis of after-action reports and other post-activity reporting from operations and other cyber support activities.

Timeline	2025–26 to 2028–29
----------	--------------------

