Australian Government
Australian Signals Directorate

ASD

ASD CORPORATE PLAN
2021–2022

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

Director-General's introduction

I, as the accountable authority of the Australian Signals Directorate (ASD), present the 2021–22 ASD Corporate Plan, which covers the period 2021–22 to 2024–25, as required under paragraph 35(1)(b) of the Public Governance, Performance and Accountability Act 2013.

ASD continues to build its foundational capabilities, structures and enterprise governance that we need as a statutory agency within the Defence portfolio, tailored to the unique nature of our work. This Corporate Plan includes, for the first time, ASD's full performance framework, including measures that will be used to evaluate ASD's performance. ASD will continue to improve its foundational capabilities over the period covered by this plan.

Our external environment is changing rapidly. The Defence Strategic Update 2020 states that "This security environment is markedly different from the relatively benign one of even four years ago, with greater potential for military miscalculation". ASD's highest priority will always be the protection of Australian lives, whether that is supporting Australia's warfighters or detecting, and in some cases disrupting, malicious threats against Australian interests.

ASD's success will depend on developing an organisation that is built around our people and the work they do, now and in the future. ASD will continue to prioritise its analyst-centric business transformation, as well as reforming our learning and development, to help our staff gain the skills required to meet emerging threats and challenges. The coronavirus (COVID-19) global pandemic has driven ASD to reflect on optimising working arrangements, including through more flexible work.

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 plan outlines the steps we will take to achieve this vision in 2021–22 and beyond.

Rachel Noble PSM
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 the Government.

ASD's purpose is achieved through the delivery of four key activities, as described in the Defence Portfolio Budget Statement 2021–22:

- 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 (PJCIS) 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 that 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.
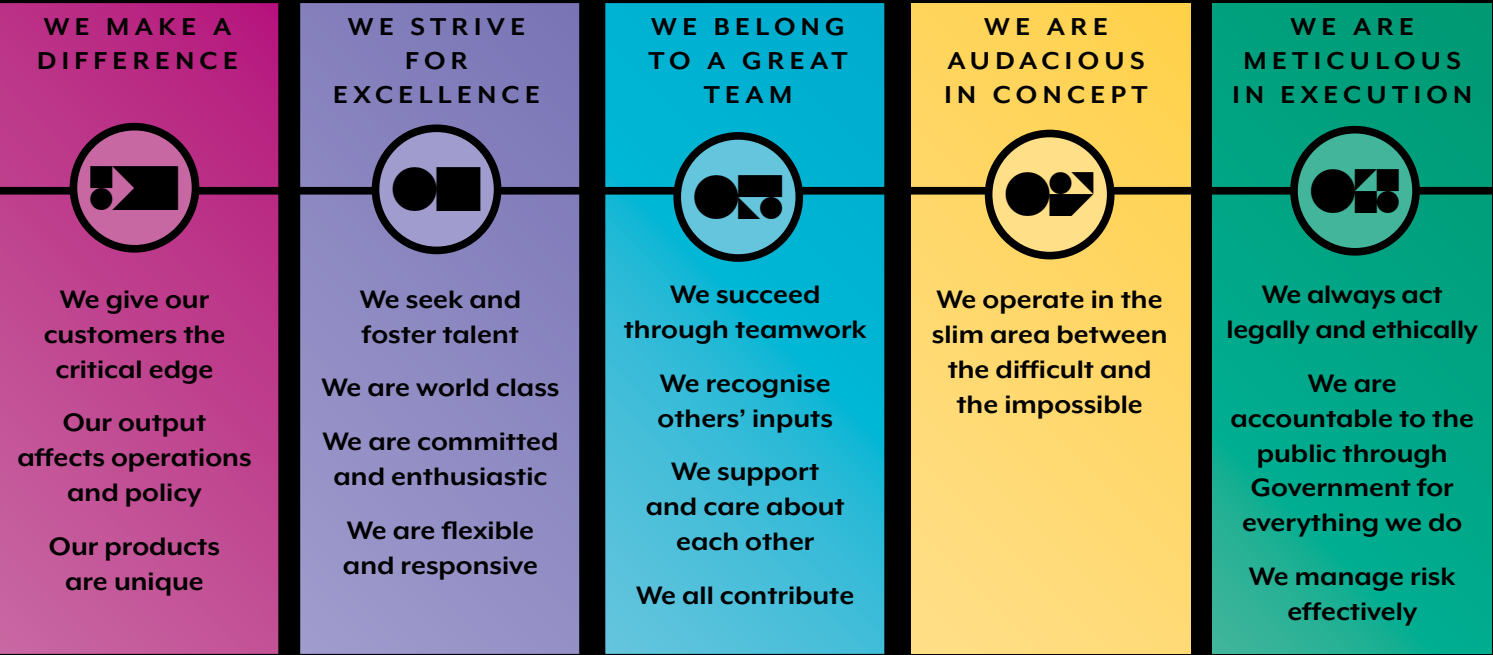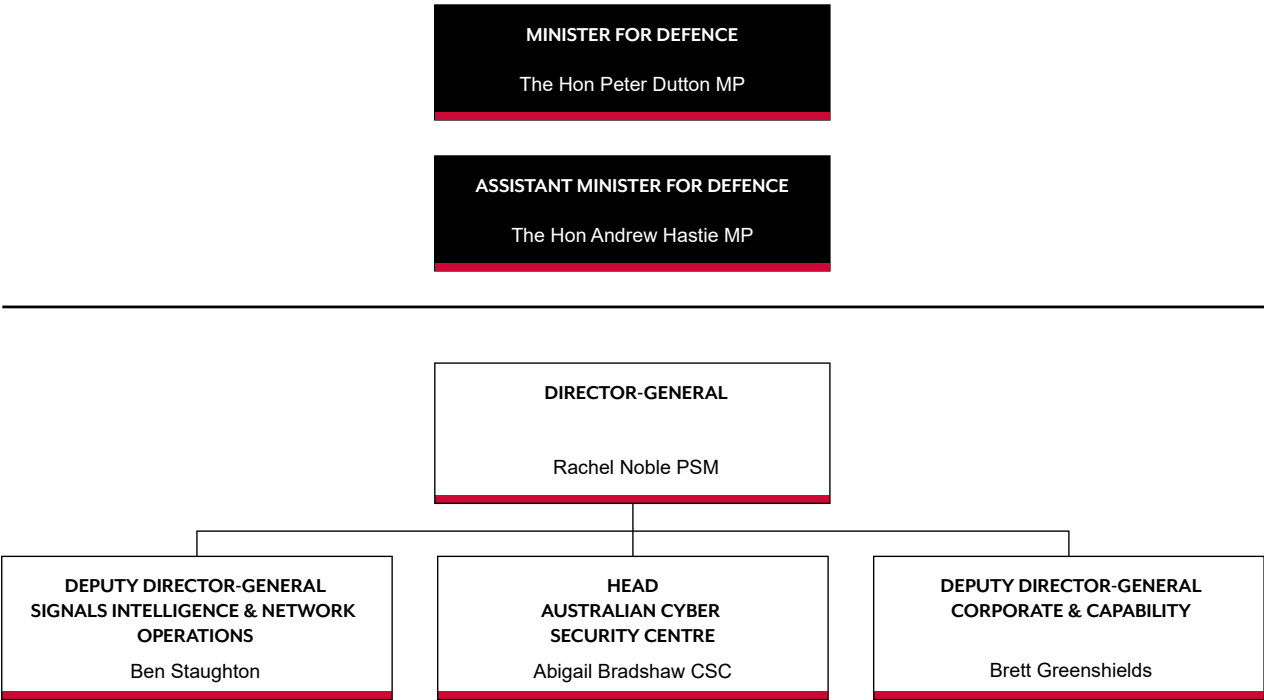
ASD's five strategic objectives

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 safest 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.

ASD VALUES

REVEAL THEIR SECRETS. PROTECT OUR OWN.

WE MAKE A DIFFERENCE

We give our customers the critical edge

Our output affects operations and policy

Our products are unique

WE STRIVE FOR EXCELLENCE

We seek and foster talent

We are world class

We are committed and enthusiastic

We are flexible and responsive

WE BELONG TO A GREAT TEAM

We succeed through teamwork

We recognise others' inputs

We support and care about each other

We all contribute

WE ARE AUDACIOUS IN CONCEPT

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

WE ARE METICULOUS IN EXECUTION

We always act legally and ethically

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

We manage risk effectively

ASD organisation chart

MINISTER FOR DEFENCE
The Hon Peter Dutton MP

ASSISTANT MINISTER FOR DEFENCE
The Hon Andrew Hastie MP

DIRECTOR-GENERAL
Rachel Noble PSM

DEPUTY DIRECTOR-GENERAL SIGNALS INTELLIGENCE & NETWORK OPERATIONS
Ben Staughton

HEAD AUSTRALIAN CYBER SECURITY CENTRE
Abigail Bradshaw CSC

DEPUTY DIRECTOR-GENERAL CORPORATE & CAPABILITY
Brett Greenshields

9

ASD STRATEGIC PLAN 2021–22 to 2024–25

CONTEXT & EXTERNAL DRIVERS

- Global Shifts
- Technological Change
- Public Trust
- Partnerships
- Fiscal Environment

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
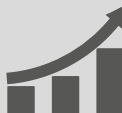
OUR VISION

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 safest place to connect online

OUR STRATEGIC OBJECTIVES

Deliver Strategic Advantage	Lead Cyber Security	Support Military Operations	Counter Cyber-enabled Threats	Provide Trusted Advice and Expertise
Generate intelligence and operational effects to protect and advance Australia's national interests	Make Australia the safest place to connect to the online world. Foster national cyber security resilience	Enable the war fighter. Protect Defence personnel and assets	Protect Australia and Australians by countering cyber-enabled crime and disrupting terrorists' use of the internet	Deliver timely, trusted and quality advice to Government, law enforcement, business and the community

OUR ENABLING CAPABILITIES

People and Culture	Technology	Partnerships	Tradecraft	Governance and Risk	Leadership and Influence
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.	We use technology in innovative and creative ways to gain asymmetric advantage. We master technology to identify and disrupt threats, and protect Australian interests.	We bring together our expertise and capabilities with those of our partners for mutual benefit. Respectful relationships and collaboration enable our success.	We give our staff the skills to solve challenging problems, and operate in the slim area between the difficult and the impossible.	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.	The leadership skills of our people underpin everything we do. And our mastery of technology underpins our trusted advice to the Government and the public.

OUR UNIQUE 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

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 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.

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 Inspector-General of Intelligence and Security (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 a significant investment in building ASD's foreign signals intelligence, cyber security and offensive cyber capabilities.

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.

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 continue to attract, develop and retain a diverse and highly skilled workforce.

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.

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.

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 is strengthening 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, neurodiversities, 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 Australian Defence Force, 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 a 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 Cyber Emergency Response Teams (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.
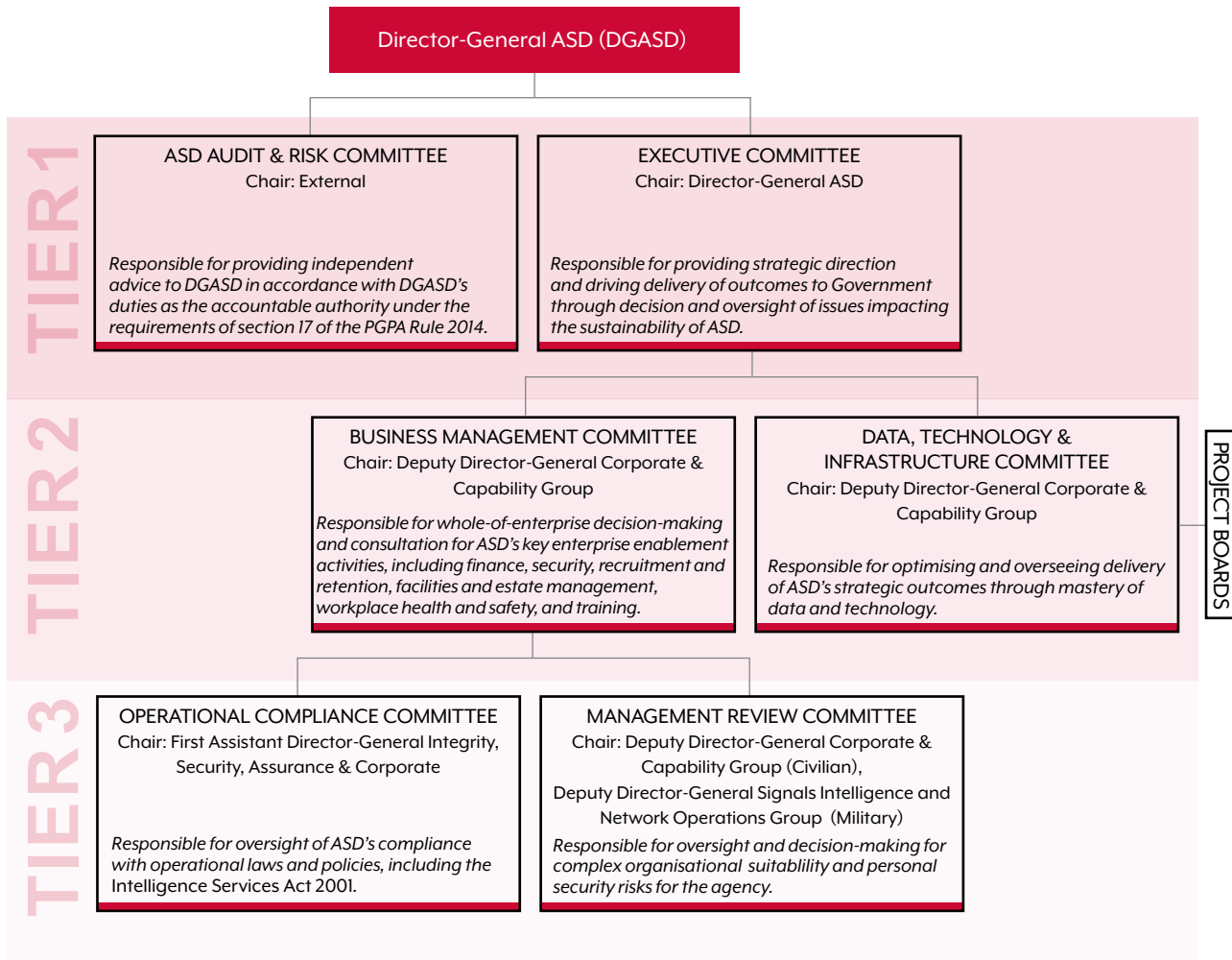
Risk oversight and management

Director-General ASD (DGASD)

TIER 1

ASD AUDIT & RISK COMMITTEE
Chair: External

Responsible for providing independent advice to DGASD in accordance with DGASD's duties as the accountable authority under the requirements of section 17 of the PGPA Rule 2014.

EXECUTIVE COMMITTEE
Chair: Director-General ASD

Responsible for providing strategic direction and driving delivery of outcomes to Government through decision and oversight of issues impacting the sustainability of ASD.

TIER 2

BUSINESS MANAGEMENT COMMITTEE
Chair: Deputy Director-General Corporate & Capability Group

Responsible for whole-of-enterprise decision-making and consultation for ASD's key enterprise enablement activities, including finance, security, recruitment and retention, facilities and estate management, workplace health and safety, and training.

DATA, TECHNOLOGY & INFRASTRUCTURE COMMITTEE
Chair: Deputy Director-General Corporate & Capability Group

Responsible for optimising and overseeing delivery of ASD's strategic outcomes through mastery of data and technology.

PROJECT BOARDS

TIER 3

OPERATIONAL COMPLIANCE COMMITTEE
Chair: First Assistant Director-General Integrity, Security, Assurance & Corporate

Responsible for oversight of ASD's compliance with operational laws and policies, including the Intelligence Services Act 2001.

MANAGEMENT REVIEW COMMITTEE
Chair: Deputy Director-General Corporate & Capability Group (Civilian),
Deputy Director-General Signals Intelligence and Network Operations Group (Military)

Responsible for oversight and decision-making for complex organisational suitability and personal security risks for the agency.

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.

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 the way in which 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.

Since ASD's establishment as a statutory agency, in July 2018, ASD has continued to develop its performance evaluation processes to ensure it effectively demonstrates the value of its activities to the Australian Government. As part of the development of this corporate plan, ASD had designed a set of 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 assessments. The performance criteria, measures, and evaluation methodology are detailed in the following tables. ASD will continue to develop its performance evaluation processes to ensure it effectively demonstrates the value of ASD's activities to the Australian Government. Due to the nature of ASD's work, some performance measures will continue to be reported through existing performance frameworks in 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 Advice and Expertise.

Key Activities

Provide Foreign Signals Intelligence	Provide Cyber Security Services	Conduct Offensive Cyber Operations	Sustain & Secure Future Capabilities
Performance Criteria			
ASD's foreign signals intelligence informs strategic, operational and tactical decision-making.	ASD's cyber security advice, assistance and operational responses prevent, detect and remediate cyber threats to Australia.	ASD's offensive cyber operations deliver real-word impact, including providing advantage to military operations.	ASD's capability needs are met and fiscal outcomes are delivered, while managing ASD's risk and maintaining a secure internal operating environment.
Performance Measures			
1. ASD meets Government's expectations to deliver strategic advantage and enables National Intelligence Community 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.	7. ASD's corporate services, and technology platforms and products' support the achievement of mission² outcomes.
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.	6. ASD's offensive cyber activities meet whole-of-government security requirements to counter offshore cyber threats.	
Performance Metrics			
1.1. ASD meets Government's 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.	7.1. ICT infrastructure support mission operations and the delivery of 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.	6.1. Offensive cyber operations that counter offshore cyber threats meet whole-of-government requirements.	7.2. ASD's workforce meets mission requirements.
2.1. ASD's foreign signals intelligence support the ADF's military operations and activities, technological advantage and capability development.	3.3. ASD's Top Secret network accreditation and key management services support stakeholders' requirements.		
	4.1. Cyber security information and expertise exchanges with partners help prevent, detect or remediate cyber threats to Australia.		
	4.2. ASD supports emerging cyber security research that may help prevent, detect or remediate cyber threats to Australia.		

Division / Branch / Individual Plans

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

ASD's performance measures

ASD continues to mature its performance framework. The performance information outlined in this corporate plan replaces the information previously published in the *Portfolio Budget Statements 2021–22*. The new performance information outlined in this corporate plan will be used as the basis for ASD's 2021–22 annual performance statements. The new performance measures better meet the guidance in section 16EA of the *Public Governance, Performance and Accountability Rule 2014*.

Performance Measure 1

PERFORMANCE CRITERIA:
ASD's foreign signals intelligence informs strategic, operational and tactical decision-making.

PERFORMANCE MEASURE:
ASD meets Government's expectations to deliver strategic advantage and enables National Intelligence Community (NIC) operations.

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
1.1	Government expectations to deliver strategic advantage are met.	NIC stakeholders confirm ASD products have a high impact³.	NIC evaluation/feedback of ASD's intelligence products, technical expertise and advice.	✓	✓	✓	✓
		Feedback from Government confirms ASD products have a high impact.	Government feedback on ASD's intelligence products, technical expertise and advice.	✓	✓	✓	✓
1.2	NIC operational requirements are met.	NIC stakeholders confirm ASD products have a high impact.	NIC evaluation/feedback on efficacy and timeliness of support to operations.	✓	✓	✓	✓
		Defence stakeholders confirm ASD products have a high impact.	Defence feedback on ASD's intelligence products, technical expertise and advice.	✓	✓	✓	✓
		NIC stakeholders confirm ASD products have a high impact.	Feedback on Requests for Information answered by ASD to support or inform NIC operations.	✓	✓	✓	✓

3 'High impact' is defined as: timely and relevant; practical, focused; provided or enabled exercisable options; and directly informed and shaped decision-making.

Performance Measure 2

PERFORMANCE CRITERIA:
ASD's foreign signals intelligence informs strategic, operational and tactical decision-making.

PERFORMANCE MEASURE:
ASD's foreign signals intelligence products and technical expertise provide effective support for military operations and **activities.**

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
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.	ADF/Defence feedback on efficiency and timeliness of ASD's intelligence products and expertise.	✓	✓	✓	✓
		ADF/Defence stakeholders confirm ASD support had a high impact.	ADF/Defence feedback on the value of ASD's intelligence products and expertise.	✓	✓	✓	✓
		ADF/Defence stakeholders confirm ASD support had a high impact.	ADF/Defence feedback on ASD's support for ADF capability advantage.	✓	✓	✓	✓

Performance Measure 3

PERFORMANCE CRITERIA:
ASD's cyber security advice, assistance and operational responses prevent, detect and remediate cyber threats to Australia.

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

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
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 times the ISM and E8 have been updated.	✓	✓	✓	✓
		Demonstrated impact.	Qualitative analysis of impact of advice and technical support provided to partners, industry and Government.	✓	✓	✓	✓
		Number of Independent Registered Assessors Program (IRAP) assessors remains constant or increases.	Number of endorsed IRAP assessors listed on cyber.gov.au.	✓	✓	✓	✓
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%.	Percentage of time cyber.gov.au is available.	✓	✓	✓	✓
			Percentage of time the ACSC Partnerships Portal is available.	✓	✓	✓	✓
			Percentage of time the 24/7 Call Centre support is available.	✓	✓	✓	✓
			Percentage of time ReportCyber is available[4].	✓	✓	✓	✓
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.	Percentage of requests for Top Secret accreditation/ certification resolved in a timely manner.	✓	✓	✓	✓
		Availability remains at or above 99%.	Percentage of time cryptographic key infrastructure is available.	✓	✓	✓	✓

4 Excluding planned maintenance.

Performance Measure 4

PERFORMANCE CRITERIA:
ASD's cyber security advice, assistance and operational responses prevent, detect and remediate cyber threats to Australia.

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

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
4.1	Cyber security information and expertise exchanges with partners help prevent, detect or remediate cyber threats to Australia.	Number of ACSC Partners increases.	Membership numbers of the ACSC Partnership Program.	✓	✓	✓	✓
		Demonstrated impact.	Qualitative analysis of impact of support to domestic partners, including Government and industry.	✓	✓	✓	✓
			Qualitative analysis impact of support to international partners.	✓	✓	✓	✓
4.2	ASD supports emerging cyber security research that may help prevent, detect or remediate cyber threats to Australia.	Demonstrated impact.	Qualitative assessment of impact of engagement to support cyber security research.	✓	✓	✓	✓

Performance Measure 5

PERFORMANCE CRITERIA:
ASD's offensive cyber operations deliver real-word impact, including providing advantage to military operations.

PERFORMANCE MEASURE:
ASD's offensive cyber operations provide effective and timely support for military operations and activities.

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
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.	ADF/Defence feedback on efficiency and timeliness of ASD's offensive cyber support to military operations and activities.	✓	✓	✓	✓
		ADF/Defence stakeholders confirm ASD support had a high impact.	ADF/Defence feedback on the value of ASD's offensive cyber support to military operations and activities.	✓	✓	✓	✓

Performance Measure 6

PERFORMANCE CRITERIA:
ASD's offensive cyber operations deliver real-word impact, including providing advantage to military operations.

PERFORMANCE MEASURE:
ASD's offensive cyber activities meet whole-of-government security requirements to counter offshore cyber threats.

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
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.	Government feedback on efficacy and timeliness of ASD's offensive cyber operations to counter offshore cyber threats.	✓	✓	✓	✓
		Defence stakeholders confirm ASD operations had a high impact.	Government feedback on the value of ASD's offensive cyber operations to counter offshore cyber threats.	✓	✓	✓	✓

Performance Measure 7

PERFORMANCE CRITERIA:
ASD's capability needs are met and fiscal outcomes are delivered, while managing ASD's risk and maintaining a secure internal operating environment.

PERFORMANCE MEASURE:
ASD's corporate services, and technology platforms and products support the achievement of mission outcomes.

	Performance Metric	Targets	Methodology (data sources measuring performance)	2021–22	2022–23	2023–24	2024–25
7.1	ICT infrastructure and services support mission operations and the delivery of corporate services.	Year-on-year improvement in service.	Qualitative analysis of stakeholder feedback regarding the provision of quality, responsive ICT service to meet mission and corporate requirements.	✓	✓	✓	✓
		ICT projects delivered to implement ASD's Enterprise Technology Strategy.	Service management statistics. Data on ICT projects delivered on time and within budget.	✓	✓	✓	✓
		24/7 ICT support for mission critical systems. Business hours support for non-mission critical systems. Available across domestic and overseas ASD sites.	Service management statistics.	✓	✓	✓	✓
		Year-on-year improvement in the percentage of systems developed within agreed interoperability standards.	Service management statistics. Data on systems developed within agreed interoperability standards.	✓	✓	✓	✓
7.2	ASD's workforce meets mission requirements.	Year-on-year improvement in delivery.	Qualitative analysis of ASD initiatives to attract and retain a skilled workforce.	✓	✓	✓	✓
		Year-on-year improvement in the percentage of staff that have met mandatory training requirements.	Defence and ASD Training System Data.	✓	✓	✓	✓
		Year-on-year improvement in the number of staff that have attended leadership and management skills courses.	ASD Training System Data.	✓	✓	✓	✓
		Year-on-year improvement in the number of staff that have attended tradecraft (customised) training courses.	ASD Training System Data.	✓	✓	✓	✓

ASD.GOV.AU