REDSPICE

A BLUEPRINT FOR GROWING ASD'S CAPABILITIES

RESILIENCE   EFFECTS   DEFENCE   SPACE   INTELLIGENCE   CYBER   ENABLERS

TABLE OF CONTENTS
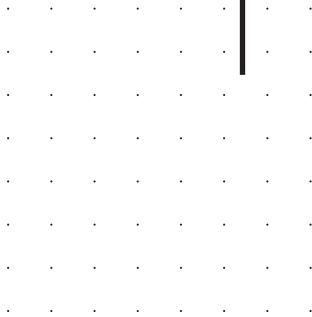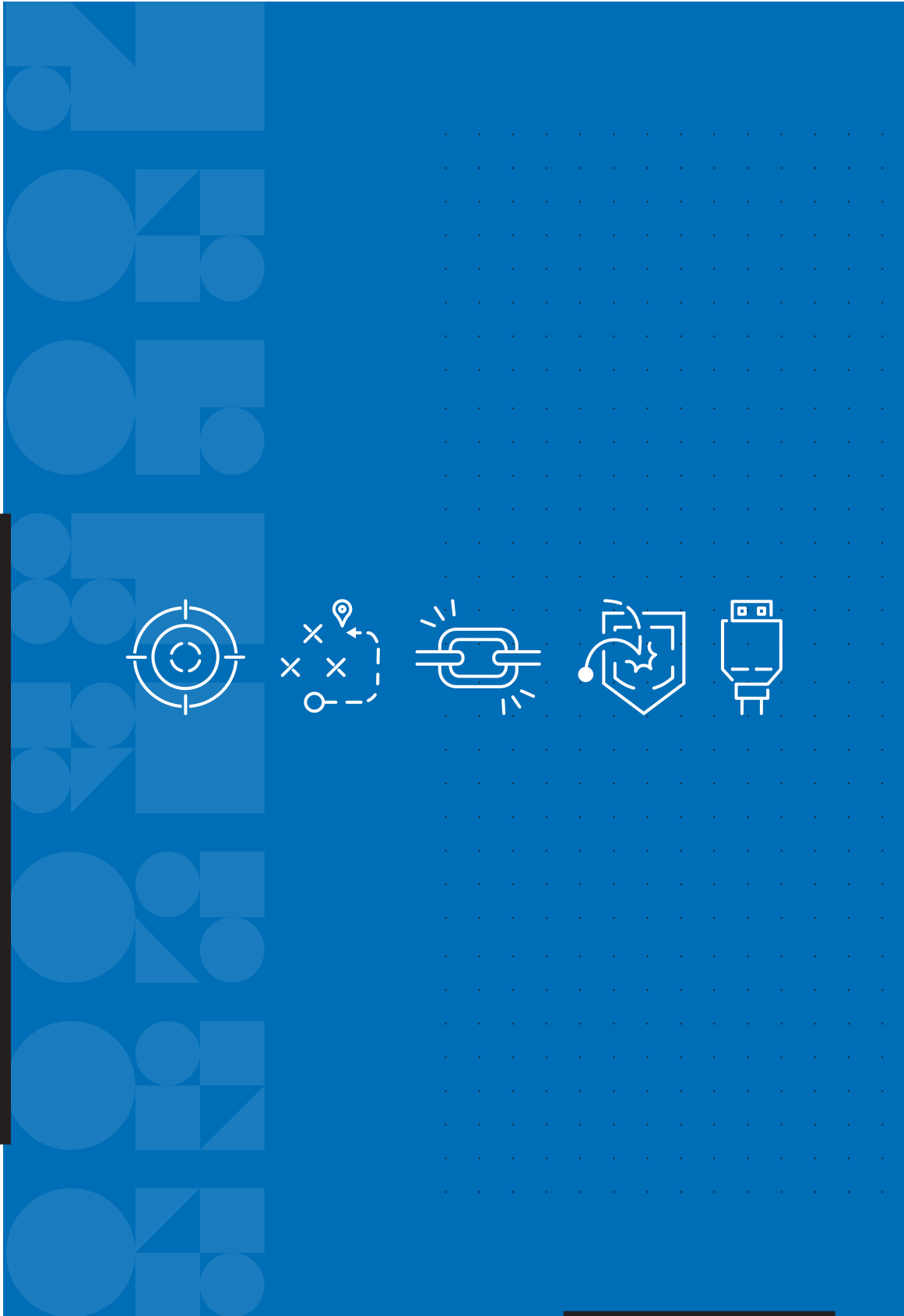
FOREWORD

Minister for Defence

The Government's firm commitment to the Australian people remains that we will keep our nation safe and protect our way of life.

Australia is well-served by our intelligence agencies. None more so than the Australian Signals Directorate (ASD).

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

Our region is in the midst of the most consequential strategic realignment since the Second World War. We are witness to rapid military expansion, increased cyber attacks, and military and economic intimidation. Technological disruption and the risk of state-on-state conflict are further complicating our nation's strategic circumstances.

The nature of warfare has also changed, with hostilities often preceded by hybrid conflicts conducted in part through aggressive or indiscriminate cyber attacks against military and civilian targets.

REDSPICE is the largest ever investment in the intelligence and cyber capabilities of ASD.
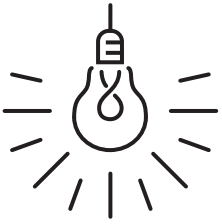
It represents the type of forward-looking capabilities that will be essential to preserve our capability edge and deliver strategic advantage for Australia over the coming decade and beyond.

It will deliver capabilities that will expand our offensive cyber arsenal, help defeat sophisticated cyber attacks, and expand the national and global footprint of ASD. It will also add to Australia's growing deterrence capability.

REDSPICE recognises that our future security depends on adapting to the changing nature of warfare. The ASD purpose and mission is more important than ever.

The Hon Peter Dutton MP
Minister for Defence

INTRODUCTION

Director-General Australian Signals Directorate

> Our mission remains audacious and our work has always made a difference. Through REDSPICE, we will transform ASD together, our future will follow our proud history.

The Australian Signals Directorate defends Australia from global threats and advances our national interests. ASD does this through the provision of foreign signals intelligence, cyber security and offensive cyber operations, as directed by Government.

Our work helps make Australia a more secure country in both peacetime and conflict.

The environment in which ASD operates is becoming increasingly challenging. Today, our region – the Indo-Pacific – is far-more complex and far-less predictable than at any time since the Second World War.

Rapidly advancing technologies present great opportunities to improve our lives, yet also pose serious threats when used against us. Throughout recent years, Australia has been targeted by a range of actors conducting cyber operations that pose a significant threat to our security.

To meet these changes in the strategic environment, ASD must continue to evolve its capabilities. We must be able to deal with increasing complexity and volume of data,

respond to new developments in technology, provide our people with the best possible tools to enable our mission, and be resilient to the environment.

REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers) is designed to respond to these challenges. It is the most significant single investment in ASD's 75-year history. REDSPICE will maintain our edge and continue to ensure that Australia is best prepared to respond to the strategic and technology environment.

This Blueprint outlines what REDSPICE will deliver. It also sets out a vision of what ASD will look like in the future.

Under REDSPICE, ASD's offensive cyber capabilities will triple, our signals intelligence capabilities will be enhanced, while growth in our defensive cyber capabilities will enable the hardening and defence of our national systems and critical infrastructure. Significantly, ASD itself will be more resilient. This will be achieved by enabling the performance of our critical functions nationally and globally.

To achieve this, ASD will grow our workforce, ensuring we have the people, technology, tools and communications to deliver our mission from multiple locations.

Our uniquely skilled workforce, values and innovative culture will be central to delivering REDSPICE. This Blueprint outlines the major skill sets ASD will continue to invest in and grow, including through 1900 new roles which include internships and traineeships.

REDSPICE is the necessary and timely change needed for ASD to continue its contribution to making Australia secure, in both peace-time and conflict. I encourage you all to familiarise yourself with it and contribute as opportunities arise.

We have a clear mandate and path to develop our future. Now more than ever the work we do is at the fore of Australia's ability to protect its interests and contribute to stability and prosperity in our region and globally.

This is an incredibly exciting time and opportunity for all of us in ASD, to evolve our organisation in ways which lay the foundation of our success for the next 75 years.

Rachel Noble PSM
Director-General
Australian Signals Directorate

REDSPICE SNAPSHOT

Through REDSPICE, we will expand the range and sophistication of our intelligence, offensive and defensive cyber capabilities, and build on our already-strong enabling foundations.

RESILIENCE

EFFECTS

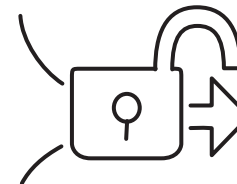**D**EFENCE

SPACE

INTELLIGENCE

CYBER

ENABLERS

3X current offensive cyber capability

2X persistent cyber-hunt activities

Advanced AI, machine learning and cloud technology

4X **global** footprint

1900 new analyst, technologist, corporate, and enabling roles across Australia and the world

40% staff located outside Canberra

OUR PURPOSE

Australian Signals Directorate Strategic Plan 2021–22 to 2024–25

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

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

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

Lead Cyber Security

Make Australia the safest 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.

Our Enabling Capabilities

People and 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.

Tradecraft

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

Partnerships

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

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.

Governance and 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 and Influence

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

OUR HISTORY

> Throughout our history, ASD has always adapted to meet changes in our environment. It is now time for us to evolve once again with REDSPICE.

ASD
ACSC

We have a proud organisational history – and will celebrate our 75th anniversary in 2022.

Our origins stretch back to WWII as part of Central Bureau attached to General MacArthur's headquarters. The Defence Signals Bureau was established on 1 April 1947. Headquartered in Melbourne, our mission was then, as it is now, to exploit foreign signals for intelligence and to ensure the security of government and military information.
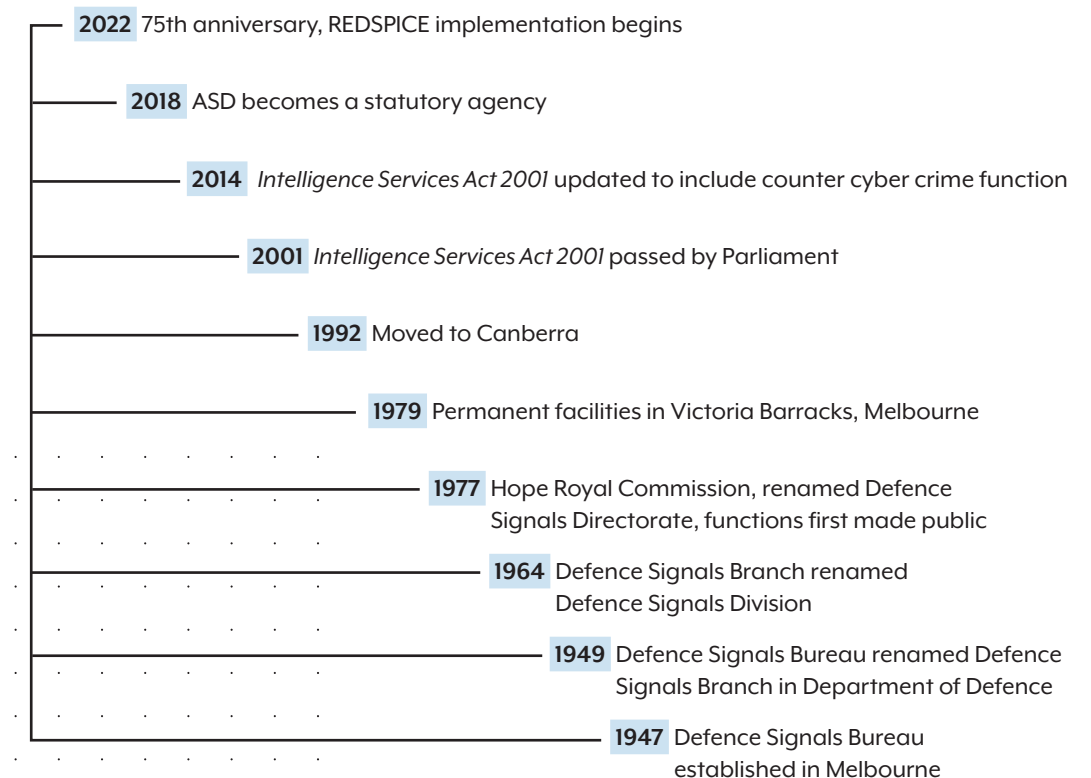
Our foreign signals intelligence role was formally acknowledged in the Prime Minister's statement to the House of Representatives on the Hope Royal Commission into Intelligence and Security in 1977. Among the outcomes of that inquiry was the renaming of the agency to the Defence Signals Directorate (DSD).
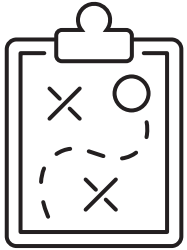
In 2001, DSD's functions and accountability framework were established in law for the first time with the passing of the *Intelligence Services Act 2001*. Our information security role was greatly expanded over this decade, driven by the seismic shift in technology and the explosive growth of the internet. In 2013, to reflect our whole-of-government role in national security and ensuring the secure use of modern technology by the government, DSD was renamed the Australian Signals Directorate (ASD).

In 2017, the Independent Review of the Intelligence Community recommended establishing ASD as a statutory authority within the Defence portfolio, and putting in place new arrangements for the Australian Cyber Security Centre.

ASD has always adapted to meet changes in our environment. It is now time for us to evolve once again, drawing on strengths that have characterised the success and culture of our organisation:

- **We have maintained a capability edge at the forefront of technology.** We acquired Australia's first supercomputer to break codes, and were an early adopter and user of 'Big Data' and Cloud technology.

- **Partnerships are at our core.** ASD's predecessor organisation, the Central Bureau – led by General MacArthur – together with our allies, brought together Navy, Army and Air Force personnel to support General MacArthur's South-West Pacific campaign by intercepting and decoding Japanese radio signals. It was truly Five-Eyes from our earliest beginnings – Australia, NZ, US, UK and Canada were all represented.

- **Flexibility in our footprint.** DSD moved from its purpose-built facility in Melbourne to co-locate with Defence Headquarters at Russell Offices, Canberra, in 1992. This facilitated closer relationships with Defence, other intelligence agencies, and key government customers. ASD also incorporated the Joint Cyber Security Centres in many state capitals.

- **People and diversity are our strength.** During WWII, women played an integral part in the work of the Fleet Radio Unit Melbourne, and the Central Bureau. In 2020, Rachel Noble became ASD's first female Director-General, and the first woman to head a statutory intelligence agency in Australia.

2022 75th anniversary, REDSPICE implementation begins

2018 ASD becomes a statutory agency

2014 *Intelligence Services Act 2001* updated to include counter cyber crime function

2001 *Intelligence Services Act 2001* passed by Parliament

1992 Moved to Canberra

1979 Permanent facilities in Victoria Barracks, Melbourne

1977 Hope Royal Commission, renamed Defence Signals Directorate, functions first made public

1964 Defence Signals Branch renamed Defence Signals Division

1949 Defence Signals Bureau renamed Defence Signals Branch in Department of Defence

1947 Defence Signals Bureau established in Melbourne

STRATEGIC ENVIRONMENT

" We need innovation, creativity, and determination to maintain our competitive edge. Our environment is constantly evolving, and so must we. Continuous improvement must be part of our DNA, as it has always been in the past. "

Director-General ASD

We are at a unique point:

The **strategic environment** is deteriorating.

The rapidly **advancing technological landscape** presents great opportunities but also serious threats.

Cyber space is of increasing importance to warfare and national security.

CHALLENGES

Strategic competition continues to increase

Competition between global powers continues to grow and regional dynamics are increasing the risk of crisis. These continue to impact Australia's interests.

Cyber capabilities continue to increase

Some countries and non-state actors are willing to use cyber capabilities maliciously to seed disinformation and destabilise economic, political and social systems and infrastructure. These capabilities are a domain of modern warfare and a tool of statecraft.

Digital technology is being used more than ever

The coronavirus pandemic underscores the importance of digital technology as an economic enabler. Millions of Australians are now working from home, staying connected through apps and using digital capabilities to deliver critical services.

Emerging and disruptive technologies are being adapted

Emerging and disruptive technologies are being rapidly assimilated into weapons systems, with proliferation of sophisticated sensors, autonomous systems, and long-range and high-speed weapons.

Coercive activities are being used

Some countries are pursuing their strategic interests through a combination of coercive activities, including espionage, interference, malicious cyber and economic levers.

Grey-zone activities are being adopted

Grey-zone activities are being adopted and integrated into statecraft. They are being applied in ways that challenge sovereignty and conventional habits of cooperation, including through a range of cyber activities. These activities impact Australia's national security interests.

Rules, norms and institutions are under strain

Rules, norms and institutions that have historically helped maintain peace, security and guidance for global cooperation are now under strain. Pressures on governance in the global environment and in domains, such as cyberspace, open up potential sources of friction.

Military modernisation is accelerating

Many countries in the Indo-Pacific are accelerating their military modernisation, enabled by a long period of economic growth. New threats include the introduction of advanced strike, maritime surveillance, and anti-access and area-denial technologies.

Major powers are being more assertive

Some of the world's major powers are seeking to advance their strategic interests and exert influence across the Indo-Pacific region. They use all elements of statecraft tools and techniques to help achieve their strategic goals.

REDSPICE SUMMARY

REDSPICE signals the start of the most significant transformation in ASD's history, investing in new intelligence and cyber capabilities.

Program

- Investing $9.9 billion over the decade, the largest ever in cyber and intelligence capabilities

- Workforce growth of 1900 over the decade

- Growing and delivering asymmetric strike capabilities and offensive cyber for the ADF

- Enabling next-generation data science and artificial intelligence (AI) capabilities

- Hardening networks against cyber attack with sharpened response capability

- Enhancing intelligence capabilities

- Improving core ASD resilience by bolstering our national and international footprint

- Providing opportunities for Australian industry, including cyber, ICT, cloud computing and enabling services.
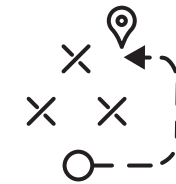
Scaled Cyber Effects
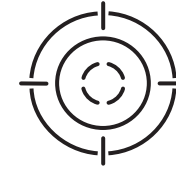
- Triples the offensive cyber effects capability to support the ADF

- Supports the integration of the ADF information warfare and cyber workforce

- Deepens technology cooperation with allies and partners

- Contributes to integrated deterrence.

New Intelligence Capabilities

- Enhances intelligence capabilities that help prevent strategic surprise, inform decisions of consequence and minimise miscalculation

- Increases understanding of adversaries' capabilities, intent and decision-making

- Doubles our analytic workforce.

Enhanced National Cyber Defence
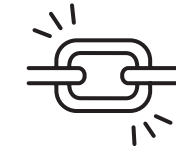
- Improves resilience of critical infrastructure against sophisticated cyber attacks

- Increases the visibility of threats to Australia's most critical systems

- Improves machine-time cyber threat intelligence sharing across government and industry

- Doubles persistent cyber-hunt activities and nationwide cyber-incident response.

Increased Resilience and Redundancy

- Increases resilience of classified communications capabilities

- Creates redundancy in critical capabilities through national and international dispersal

- Employs 40% of ASD workforce outside of Canberra

- Increases our overseas footprint fourfold.

Improved Foundational Technologies

- Delivers new cloud-based cyber and intelligence systems and applications

- Scales up AI and machine learning capabilities

- Delivers AI-supported offensive and defensive cyber capabilities.

OUR PEOPLE

We belong to a great team.

Delivering REDSPICE will rely on our people. Our uniquely skilled workforce, and innovative and inclusive culture, is at the heart of ASD. Our team is located around Australia and the globe, working side-by-side with our partners and allies. We have a diverse, agile and integrated workforce that is supported to deliver the ASD Mission.

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.

Details of our signals intelligence and cyber capabilities are necessarily secret. However, the roles required by those capabilities are not secret.

We need a broad range of skills that encompasses **analyst** and **technologist roles,** as well as **corporate and enabling services.**

> We work with clever, inquisitive people skilled in problem solving and creative approaches.
> If this is you, then we are interested.
> Go to: **asd.gov.au/careers**
>
> There are many ways you can join us: Entry level Programs, Graduates, Apprentices, Cadets and Interns.

Who ASD needs to realise REDSPICE:

Analysts

Create our edge, solve the problems others cannot.

- Analyse communications systems and foreign signals intelligence
- Understand targets, their intent and capabilities
- Develop new methods of analysing and exploiting data
- Investigate large and complex data sets
- Prepare intelligence products for government and allies
- Develop and implement policies that enable legal and compliant activities
- Protect Australia from cyber adversaries as part of the Australian Cyber Security Centre (ACSC)
- Solve cryptological problems using advanced mathematics
- Translate, analyse and report target communications
- Plan and conduct offensive cyber operations to counter cyber crime and support the ADF
- Conduct covert online operations to enable intel, cyber security and offensive cyber outcomes.
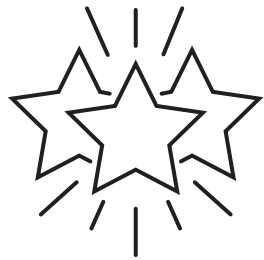
Technologists

Use emerging and cutting-edge technology and big data to solve complex problems.

- Develop capabilities using software development skills to support intelligence and cyber outcomes
- Perform forensic analysis and intrusion detection to protect and defend national interests
- Conduct reverse engineering on malicious software
- Perform system administration and maintenance to ensure the security of complex networks, systems and databases
- Think critically to design and test systems and architecture to achieve maximum capability impacts.

Corporate & Enabling Services

Enable our purpose.

- Manage the programs and projects that enable and deliver capability
- Ensure our workforce has fit-for-purpose facilities
- Deliver the ICT services that form the backbone of enterprise performance
- Develop/maintain human resources, learning, development, and training for a dynamic, specialised, diverse and technical workforce
- Deliver the specialised psychology and security services that are a vital part of Australia's intelligence community
- Ensure the services of legal counsel
- Develop policies and materials to support ASD's international partnerships.

IMPLEMENTING REDSPICE

We will:

Change at scale and speed

The gravity of change in our strategic and technology environment sets the context for the scope, scale and delivery speed of REDSPICE. We will move rapidly, but deliberately, to ensure we maintain our capability edge. We will remain consistent with existing business transformation activities – such as our program to deepen analyst expertise and modernise analysis systems – and will reform our learning and development capabilities to help our staff gain and maintain the skills required to meet emerging threats and challenges.

Draw on our culture and values and be OneASD

Our culture of collegiality, collaboration and continuous improvement is the key to maintaining our unique and rewarding workplace culture. We will pursue this transformation together, with our 'One ASD' approach at the core.

Engage as we evolve

Our people will be engaged and supported to participate and shape the changes resulting from this investment. We will inform, update, listen, learn and iterate.

Collaborate

We will collaborate across industry, academia, government and with allies to deliver capability. We leverage partnerships to drive success.

Governance

ASD will use existing governance mechanisms, augmented by a dedicated REDSPICE Program Board and External Advisory Board.

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 CONNECTIONS

National Intelligence Community

- Coordinated approach to workforce growth
- New cloud capabilities
- New national facilities

Public

- Enhanced national resilience in protecting critical infrastructure
- New employment opportunities nationally and globally

Industry

- $5 billion in opportunities for Australian industry
- A focus on sovereign capability
- Expanded partnerships with industry
- New higher education partnerships
- Investment in key sectors including AI, cyber, ICT and engineering

5-Eyes

- Greater integration through expanded global footprint
- Co-investment in Five-Eyes initiatives
- Collaboration on AI and cyber technologies

ADF

- Improved intelligence support to ADF
- Enhanced offensive cyber capabilities to support the ADF
- Integrated with ADF information warfare workforce
- Hardened networks and systems.

INDUSTRY OPPORTUNITIES

There are a range of opportunities for industry.

REDSPICE provides $5 billion in opportunities for Australian industry, including small and medium Australian enterprises.

We will rely heavily on Australian expertise and technology to deliver cyber security, telecommunication and cloud computing components, and for strategic partnerships to deliver workforce and facility solutions.

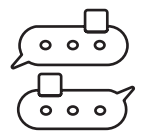Examples of Australian industry partnership opportunities are:

Software-enabled capabilities to prevent network exploitation and deliver network effects	ICT programs and cloud technologies, including multi-classification	Delivery of facilities and office fit outs	New and hardened secure comms
Strategic partnerships to deliver workforce planning, recruitment and training	Program management, change and transformation management	ICT hardware infrastructure	AI and machine learning technology and data services

EXPRESSING YOUR INTEREST

Contact us at **asd.assist@defence.gov.au**

Register at **marketplace.service.gov.au** or **business.gov.au/odis**