



Australian Government
Australian Signals Directorate



ASD & INDUSTRY

PATHWAYS TO ENGAGING WITH ASD FOR CAPABILITY DELIVERY

EFFECTS

DEFENCE

SPACE

INTELLIGENCE

CYBER

ENABLERS

TABLE OF CONTENTS

Introduction	2
Our purpose	4
ASD transformation	6
What are we doing?	8
A spotlight on REDSPICE	9
Who do we need?	10
The benefits of working with ASD.	11
Where do you fit?	12
Where do we operate?	14
Next steps	16
The Defence Industry Security Program	17
ASD procurement and approach to market	18
Keep in touch	19
Further information & support.	20

INTRODUCTION

Director-General Australian Signals Directorate

The Australian Signals Directorate (ASD), defends Australia from global threats and advances our national interests. ASD does this by providing 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.

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. We are seeing coercive activities being used below the threshold of traditional conflict and, therefore, to detect and respond to those threats, ASD's unique expertise and capabilities are becoming more important.

Australia continues to be targeted by a range of actors conducting cyber operations that pose a significant threat to our security. To meet this threat, it is critical we operate our signals intelligence, offensive and defensive cyber levers seamlessly and at scale.

ASD, through its 75-year history, has always pursued a capability edge to remain at the forefront of technology. We acquired Australia's first supercomputer to break codes, and were an early adopter and user of 'Big Data' technologies.

ASD 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 threat environment.

ASD delivers on multiple programs in the Defence Integrated Investment Program with the biggest of these being REDSPICE.

REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers), ASD's \$9.9 billion investment program, is designed to respond to the challenges we face at accelerated speed and scale. For ASD to achieve REDSPICE, the resourcefulness and expertise of trusted industry partners is critical.

ASD is invested in strengthening existing partnerships with industry and forging new ones with providers who have leading edge capabilities that are scalable, adaptable and sustainable to support in confronting the challenges our complex environment brings.

The industry opportunities with ASD are significant. They span the breadth of our work in access, data, collection and processing, operations, intelligence production, enhanced national cyber defence, resilience and corporate services.

The industry opportunities with ASD are significant. They span the breadth of our work in access, data, collection and processing, operations, intelligence production, enhanced national cyber defence, resilience and corporate services.

Industry is central to our ambition to elevate capability, which will see ASD:

- uplift offensive cyber to support the ADF, cyber workforce and deepen technology cooperation with allies
- enhance intelligence capabilities to help prevent strategic surprise; inform decision-making and minimise miscalculation
- improve resilience of critical infrastructure against sophisticated cyber-attacks and increase the visibility of threats to our most critical systems
- increase the resilience of classified communications capabilities, with investment in cloud-based cyber and intelligence systems and applications and
- expand our national presence, which includes an interstate workforce.

Together we can make Australia a more secure country.

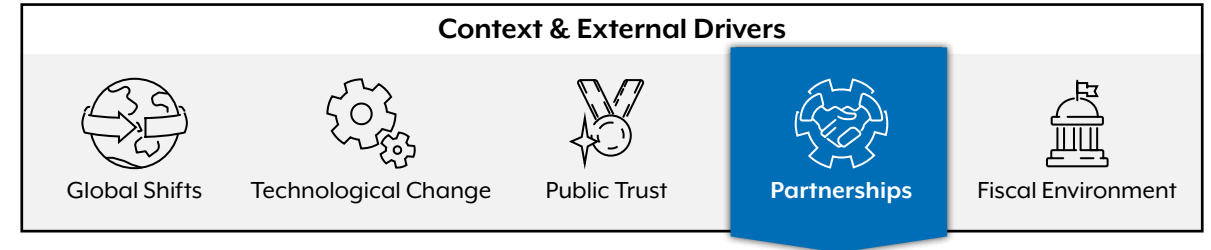


Rachel Noble PSM
Director-General
Australian Signals Directorate

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.



Our Vision

We are a world-class intelligence, covert effects and cyber security **strong partnerships**, and the trust of the Australian public. Our **trusted advice** and to conduct intelligence operations.

agency, enabled by talented and dedicated people, leading-edge capabilities, role as both 'poacher' and 'gamekeeper' uniquely positions us to provide

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 war fighter. 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

ASD

TRANSFORMATION



Our Strategic Objectives →

Deliver Strategic Advantage

Additional intelligence missions and uplift of ASD's offensive cyber capability to protect and advance Australia's national interests.

Lead Cyber Security

Fosters national cyber security resilience by doubling persistent cyber-hunt activities, increasing threat visibility, and improves resilience of critical infrastructure.

Support to Military Operations

Supports the integration of a growing ADF information warfare and cyber workforce, contributing to integrated deterrence.

Counter Cyber-Enabled Threats

Improves machine-time cyber threat intelligence sharing and delivers new cloud-based cyber and intelligence systems, and artificial intelligence (AI) supported defensive cyber capabilities.

Provide Trusted Advice & Expertise

Deepens technology cooperation with allies and partners and focuses on improving foundational technologies, scaling up AI and machine learning capabilities.

Capability Uplift

The REDSPICE Organisational Transformation

People & Culture

ASD will employ 1900 new people outside of Canberra and create resilience in critical capabilities across Australia. ASD will embrace work across all security classifications.

Tradecraft

Significant investment in training and upskilling of analytic and technical roles to ensure staff are equipped and resourced to deliver our strategic objectives.

Partnerships

REDSPICE alone provides opportunities for Australian industry (approx. \$5b) and increases our overseas footprint fourfold.

Technology

Our capability programs enable ASD to remain leading edge by connecting with innovation and participating in the development of next-generation technologies.

Governance & Risk

ASD is best postured to deliver through strong governance and risk structures.

Leadership & Influence

ASD is committed to strengthening leadership and development programs to ensure the success of ASD and grow our future leaders.



Our Enabling Capabilities →

WHAT ARE WE DOING?

Across all programs, ASD will uplift capability with industry in the following areas:

- software applications to enable network exploitation and deliver network effects
- ICT hardware, software and sustainment services
- artificial intelligence exploration and analytic applications
- data science services
- new and hardened secure communications capabilities
- secure cloud-based systems and applications
- networks and systems administration support
- Science, Technology, Engineering and Mathematics (STEM) training and upskilling
- research and development in emerging technology
- collaborative technical and information sharing partnerships
- program delivery that supports strategy, change and transformation management, consulting, workforce planning, recruitment and finance
- learning and development
- strategic communications support
- delivery of facilities, office fit-outs, maintenance, property and infrastructure services.

A SPOTLIGHT ON REDSPICE

REDSPICE is a **\$9.9 billion** investment.

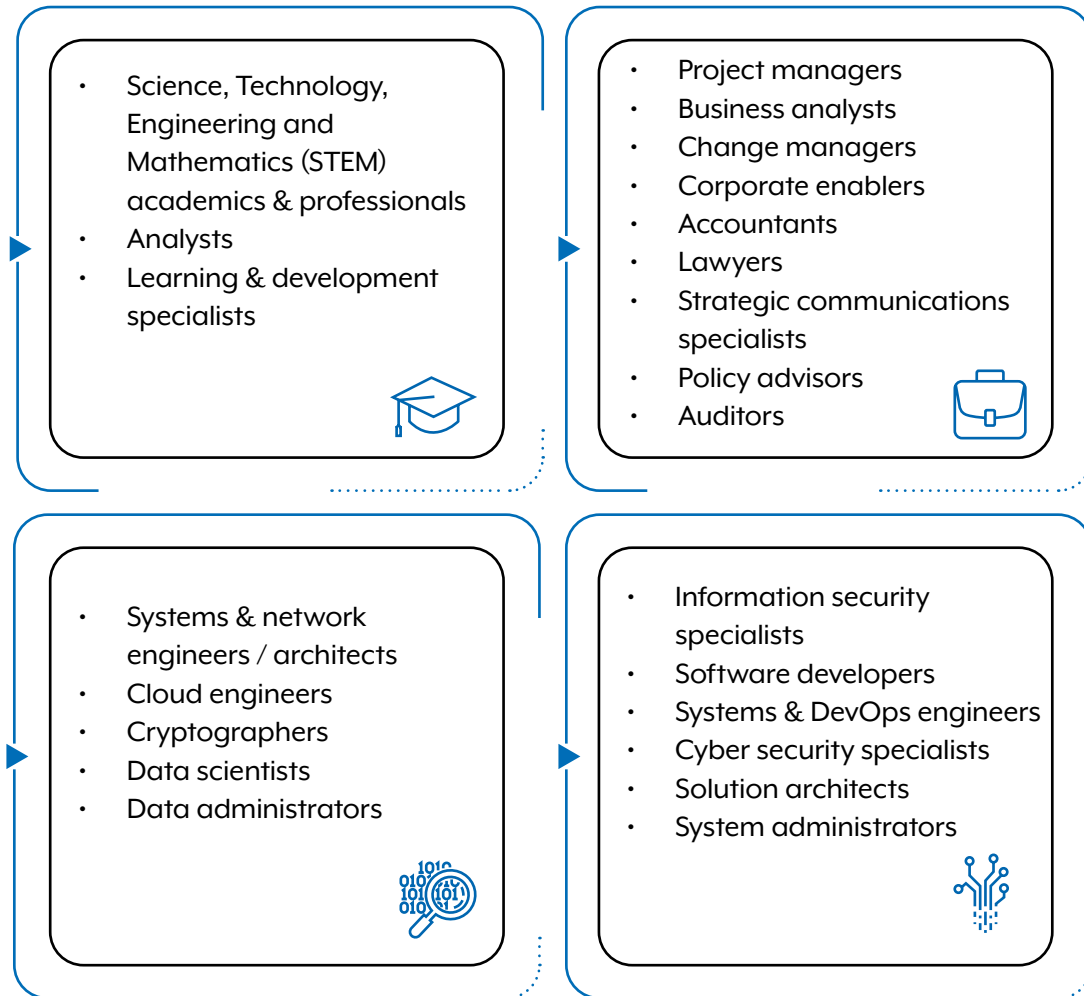
Through REDSPICE, ASD is delivering **forward-looking capabilities** essential to maintaining Australia's strategic advantage and technology edge over the coming decade.

ASD is **looking to industry** for products, services and personnel to support REDSPICE.

REDSPICE will deliver all capabilities by 2027.

WHO DO WE NEED?

To research, plan, build, deliver and sustain capability, we need support from industry. These are the critical support roles and talent we need to assist us in capability development and integration in order to achieve our goals:



ASD will approach the market for these skill sets to assist us with developing and/or delivering capability.

THE BENEFITS OF WORKING WITH ASD

- Help protect and enhance Australia's national security.
- Be part of and contribute to scaling Australia's sovereign technological capability.
- Assist in solving ASD's complex and difficult problems in areas that include the future of artificial intelligence, cloud, quantum, secure communications and scaled cyber effects.
- Receive investment into your innovative ideas, products and services.
- Support national critical infrastructure uplift.
- Have access to ongoing contractual opportunities within the national security community.
- Have access to vetted workforce opportunities.
- Participate in opportunities to collaborate and network with other like-minded industry partners.
- Help make a difference.

WHERE DO YOU FIT?

- ▶ Ideas
- ▶ Research and development
- ▶ Problem solving
- ▶ Pilot programs

ASD operates in the slim area between the difficult and the impossible and succeeds through innovation and improvement. We want to hear about your innovative idea, or know if you are working in technological and futuristic fields and can help us solve technical problems. We want to work with academia, research institutes, think-tanks and companies.

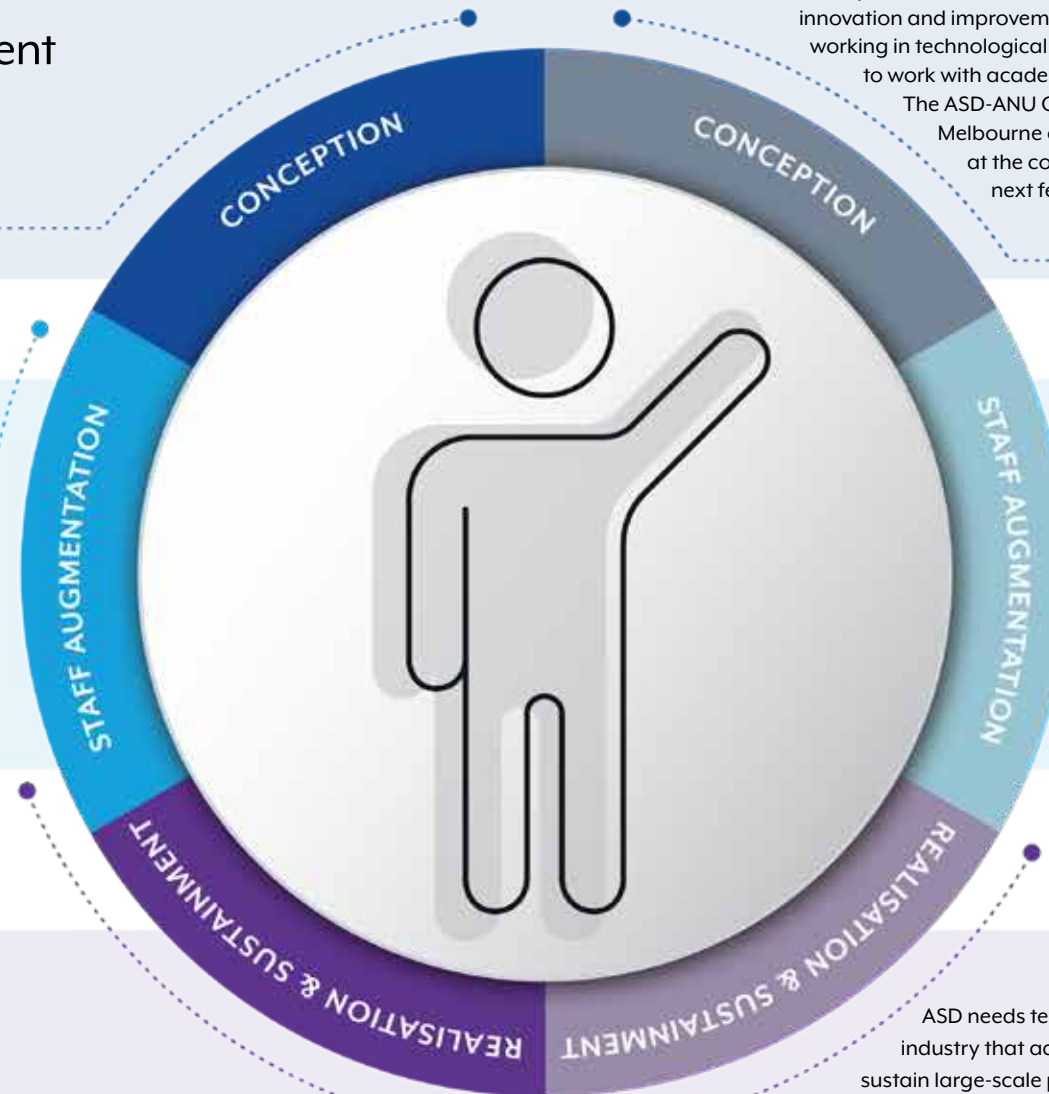
The ASD-ANU Co-Lab in Canberra and the establishment of the AI/ML Hub in Melbourne are examples of where ASD is exploring emerging technology and ideas at the conception stage. ASD will be investing more into conception over the next few years.

- ▶ Projects
- ▶ Skilled professional workforce
- ▶ Procurements

ASD operates a high-security environment. We need security-cleared professionals and talented people to help us develop and deliver capability. We access security-cleared contractors through channels like the Technical Support Services (TSS) Standing Offer Panel and other official government procurement systems. As we continue to grow our presence across Australia in Melbourne, Brisbane and Perth, we need security-cleared personnel and industry to support our capability developments in these regions.

- ▶ Complex procurements
- ▶ Long-term projects

ASD needs technically advanced and capable organisations operating in the defence industry that adhere to our security requirements in order to help us deliver and sustain large-scale projects. An example includes the Strategic Industry Partnership (SIP) Arrangement Panel for people and complex capability delivery. We need organisations that can help ASD define, acquire and integrate capability across major projects and assist us with strategic implementation. ASD uses official government procurement systems to source industry expertise.



WHERE DO WE OPERATE?

THE AUSTRALIAN SIGNALS DIRECTORATE (ASD)

ASD headquarters is located in Canberra. Under REDSPICE, we are growing our national presence with new large ASD facilities in Brisbane, Melbourne and Perth. We want to engage with industry across our national footprint.

THE ASD CYBER SECURITY PARTNERSHIP PROGRAM

ASD has state and territory presence around the country and runs the ASD Cyber Security Partnership Program so that industry can exchange technical information and engage on cyber security to increase national cyber resilience. To join the ASD Cyber Security Partnership Program visit www.cyber.gov.au

INTERNATIONAL

As part of the Five-Eyes community, ASD engages with industry and stakeholders who are working with our counterparts internationally.



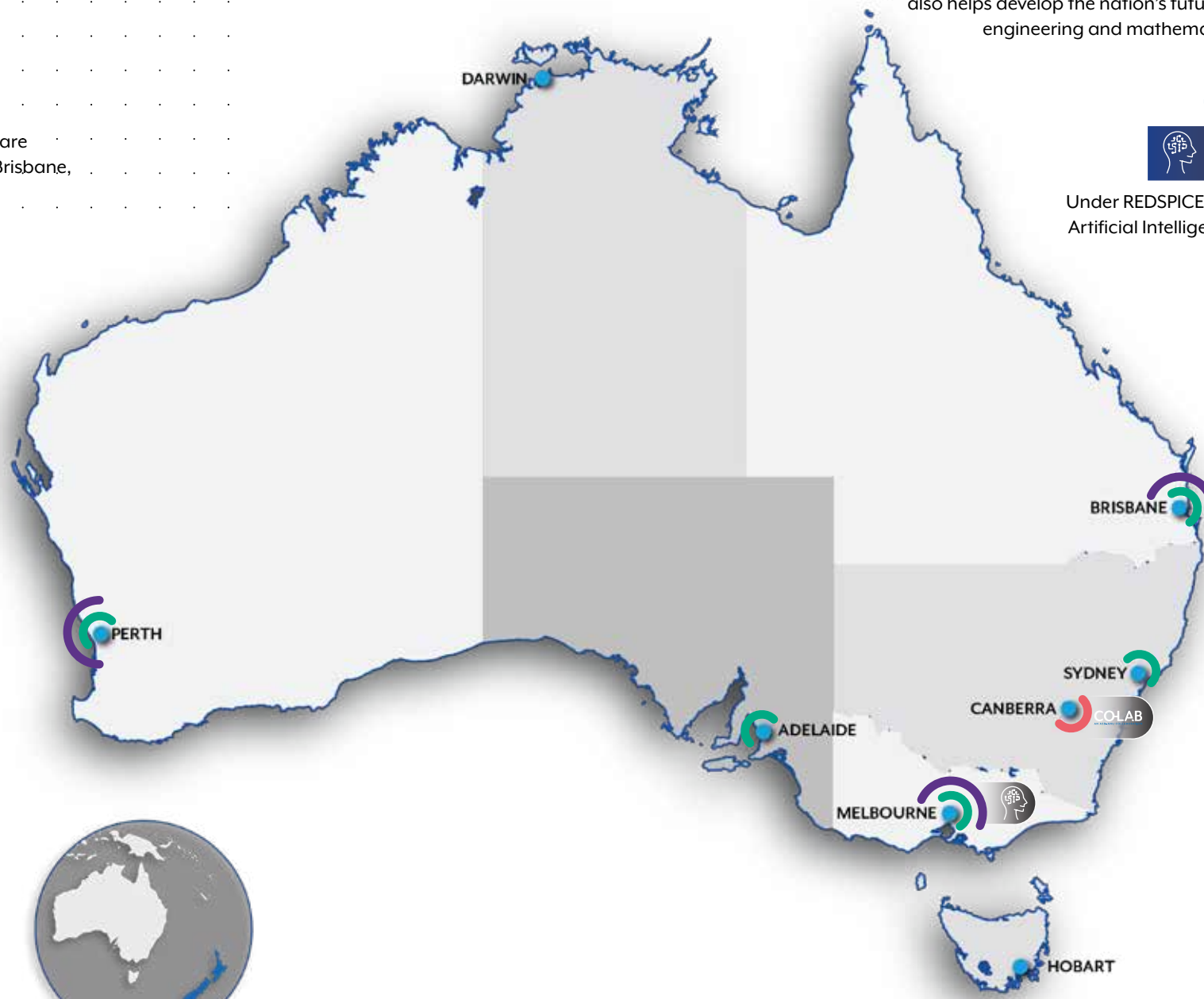
Canada
United States



United Kingdom



New Zealand



COLAB ASD-ANU CO-LAB
Located in Canberra

The **ASD-ANU Co-Lab**, is a collaborative research partnership between ASD and the Australian National University (ANU). The Co-Lab is an example of how ASD is partnering to conduct complex research into Australia's toughest national security problems. The Co-Lab also helps develop the nation's future science, technology, engineering and mathematics (STEM) workforce.

AI HUB
Located in Melbourne

Under REDSPICE, ASD is establishing an Artificial Intelligence Hub in Melbourne.

ASD State Offices ASD Headquarters New ASD Facilities

NEXT STEPS

*Have a great product and/or great people?
Consider these things to work with us in our environment:*

Security Responsibilities

Defence industry and associated research and technology sectors are known targets for foreign intelligence services, regardless of their relationship with Australia.

To do business with ASD, industry needs to adhere to a number of physical, personnel and information/ICT security responsibilities. Those engaged on a project may need to obtain and maintain a national security clearance.

Cyber Responsibilities

Industry will need to adhere to cyber security assurance and will be required to uphold one of the cyber security accreditation standards:

1. ACSC Essential Eight
2. NIST SP 800-171
3. Def Stan 05-138
4. ISO/IEC 27001 and 27002

Further information is provided through the Defence Industry Security Program (DISP).

To work with us, it is advised that industry join the ASD Cyber Security Partnership Program. Additional guidance and resources on the Partnership Program, cyber uplift and support services like the InfoSec Registered Assessors Program (IRAP), an ASD-endorsed qualified cyber security professional assessment service, can be found on www.cyber.gov.au

Whilst the IRAP assessment is not a requirement for Defence accreditation under DISP membership, the Assessment can help inform decisions to authorise systems storing, processing or transmitting Australian Government information at PROTECTED level and above under the Australian Government Protective Security Policy Framework (PSPF).



Australian Government

Defence

THE DEFENCE INDUSTRY SECURITY PROGRAM

The Defence Industry Security Program (DISP) sets baseline security requirements for industry wishing to engage in Defence projects, contracts and tenders.

Becoming a DISP member will enable access to long-term capability delivery opportunities within ASD.

DISP supports industry to identify security risks and to understand and apply security controls across the domains of governance, personnel security, physical security, information and cyber security.

DISP membership is open to any Australian business looking to become a part of the defence industry supply chain. You do not require a contract with Defence to become a member of DISP.

The Defence Industry Security Office (DISO) manages the DISP.

SUPPORT

Further information on DISP can be found at www.defence.gov.au/dsvs/industry

Key government security policies and guidelines can be found on page 20.



ASD PROCUREMENT AND APPROACH TO MARKET

So you're ready to work with us...

ASD operates under the *Public Governance Performance and Accountability Act 2013* (PGPA Act), the *PGPA Rule 2014* and the *Commonwealth Procurement Rules* (CPRs). The PGPA Act and PGPA Rule provide the general legal framework that government officials must follow when undertaking a procurement. The CPRs provide detailed instructions to officials undertaking procurements and making value-for-money assessments.

ASD's procurement approach recognises and supports:

Australian industry small and medium-sized enterprises (SMEs)	The Indigenous Procurement Policy (IPP)	Sovereign capability development
---	---	----------------------------------

ASD uses many avenues to approach industry.

ASD will advertise industry opportunities for people, products and services through official government procurement channels. These include:

Austender

The procurement information system operated by the Australian Government www.tenders.gov.au

BuyICT

The online marketplace that connects government buyers with ICT industry suppliers www.buyict.gov.au

Standing Offers

ASD engages a number of panels. In a panel arrangement, suppliers have been appointed to supply goods or services for a set period of time under agreed terms and conditions, including agreed pricing. ASD also welcomes sub-contracting arrangements where industry are not panel members.

Further information on panels can also be found on the Austender website www.tenders.gov.au

Advanced Strategic Capabilities Accelerator (ASCA)

ASD will work closely with the Department of Defence to access and engage with innovative technologies.

KEEP IN TOUCH

Partner with the ASD Cyber Security Partnership Program

The ASD Cyber Security Partnership Program enables Australian organisations and individuals to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy in a non-commercial setting.

For further information on the Partnership Program, please visit www.cyber.gov.au

If you are a member of the Partnership Program, you can also reach out to your ASD state office for further information on collaboration, partnerships and networking opportunities.

For all general enquiries asd.assist@defence.gov.au



FURTHER INFORMATION & SUPPORT



The Office of Defence Industry Support (ODIS) assists eligible businesses working or seeking to work in the defence industry.

Further information around working with Defence can be found at: www.business.gov.au/odis

Have an innovative idea that can enhance Australia's Defence capability?

The Advanced Strategic Capabilities Accelerator is a new entity in Defence that drives innovation to create capability for the Australian Defence Force.

Further information can be obtained through asca.enquiries@defence.gov.au

Looking to become a Defence Industry Security Program (DISP) member?

For further information, please contact DISP directly through www.defence.gov.au/security/industry

Key government security policies and guidelines:

- Protective Security Policy Framework (PSPF) by the Attorney General's Department www.protectivesecurity.gov.au
- Defence Security Principles Framework (DSPF) www.defence.gov.au/security
- The Australian Government Information Security Manual (ISM) www.cyber.gov.au

Further cyber security guidance, information on the ASD Cyber Security Partnership Program and the InfoSec Registered Assessors Program (IRAP), can be found at www.cyber.gov.au

Please note that opportunities to work with ASD will require adherence to security responsibilities. DISP membership, along with certification and accreditation against the policies mentioned above are recommended.

For further detail on ASD, please visit www.asd.gov.au

ASD

The logo graphic consists of a series of white shapes: a solid circle on the left, followed by a square with a smaller square inside, then a square with a circle inside, then a solid circle, and finally a square with a smaller square inside on the right.