



Australian Government
Department of Defence



SOVEREIGN INDUSTRIAL CAPABILITY PRIORITY INDUSTRY PLAN

Advanced signal processing

December 2020





SECRETARY OF DEFENCE AND CHIEF OF THE DEFENCE FORCE FOREWORD

We are pleased to release the *Advanced signal processing* Industry Plan, a key deliverable of the *2018 Defence Industrial Capability Plan*.

Advanced signal processing technologies are critical tactical capabilities that enable the Australian Defence Force (ADF) to: rapidly assess the operating environment; to identify potential threats; avoid detection from any potential adversary; and to disrupt their critical systems while protecting our own. The importance of these capabilities highlights the nature of modern warfare, where control of the information domain leads to control of the battlespace. As strategic competition and uncertainty intensifies, Australia must have the most advanced signal processing capabilities to enable us to see and shape the modern battlespace, deter our adversaries from acting against our interests, and to respond as required.

The ability to identify and track potential threats in battle—while also remaining hidden from adversaries—is critical for the warfighter. However, achieving this outcome has become progressively more difficult with an increasingly congested electromagnetic spectrum, and technological advancements in sensor processing and signature management. Recognising advanced signal processing as a Sovereign Industrial Capability Priority highlights the changing nature of warfare, and emphasises the significance of this technology in generating warfighting advantage – now and into the future.

Through close consultation with experts from industry and Defence, we have identified the critical industrial capabilities that must be delivered or supported by Australian industry. Australia needs access to, or control over, these capabilities to ensure we can meet our current and future needs. Encouraging innovation and agility in the defence industry sector ensures Australia can meet the challenge of rapid technological refresh that comes with this capability and the changing security environment. COVID-19 has highlighted the importance of secure supply chains. It is crucial that we build sovereign capability in the critical industrial capabilities outlined in this Plan.

This Plan—which should be read in conjunction with the Surveillance and intelligence Industry Plan—outlines the skills and capabilities needed within industry to maintain and enhance the ADF's advanced signal processing capabilities. We recognise Australian industry and our international allies are key partners in this endeavour, and this Plan helps shape investment and increase our sovereignty.

The Plan identifies many of the skills and capabilities underpinning these technologies and their broader applications. This Plan helps businesses seeking to diversify their customer base to move into this sector of defence industry.

Many defence industry representatives and Defence personnel volunteered their time and expertise to develop and strengthen this Plan, and we thank them. As we continue to build and strengthen our partnership, we will secure a sovereign industrial base that ensures access to the most critical industrial capabilities underpinning Australia's defence preparedness.



Greg Moriarty
Secretary
December 2020



Angus J Campbell, AO, DSC
General
Chief of the Defence Force
December 2020



The Government's *2018 Defence Industrial Capability Plan* identified the first 10 Sovereign Industrial Capability Priorities. These priorities are critical to Defence and must be developed or supported by Australian industry.

These Industry Plans, as well as the overarching Implementation Plans, build on the *Defence Industrial Capability Plan* to identify the critical industrial capabilities that underpin each priority. They enable informed and timely defence capability decisions. To protect its sovereign interests, Australia requires a level of access to – or control over – essential skills, technology, intellectual property, financial resources and infrastructure within the Australian defence industrial base. This level of access or control will enable Australian industry to realise the benefits associated with these interests. This Industry Plan enables both Defence and industry to better understand those opportunities and the trade-offs associated with sovereign capability. It should be read in conjunction with the Implementation Plan.

Guidance for Government Readers:

This Industry Plan supports Government, Defence project managers and others involved in capability acquisition and sustainment. This Plan provides information and guidance to enable Defence to align capability decisions with the strategic intent of the department and broader whole-of-government policies, including:

- The critical industrial capabilities to be developed in Australia to support this Priority (pages 6, 20–21).
- The capability enablers required to protect Australian sovereign interests (pages 34–36). This information will support industry's business planning and investment decisions, as well as enable the development of Australian Industry Capability Plans that align with Defence priorities.
- A description of the industrial base and its dynamic to support planning and consultation, including preparing for and undertaking market solicitation, such as requests for information (pages 23–33).
- The actions to be taken by government to support development of this Priority (pages 34–36 and consolidated in Annex A).

Guidance for Industry Readers:

This Industry Plan details specific areas of focus for Defence, enabling industry sovereign capability by investing in those capabilities identified as critical (for example in workforce, technology or infrastructure). The Plan includes:

- An explanation of the policy environment, and a definition of defence sovereignty and what it means to be a Priority (pages 10–11).
 - The critical industrial capabilities and capability enablers related to this Priority, and Defence's intent to access or control particular aspects (pages 6, 20–21). This will support industry's business planning and investment decisions, as well as enable Australian Industry Capability Plans to be developed that align with Defence priorities.
 - A description of the industrial base and its dynamics, highlighting barriers and opportunities in the supply chain for this Priority. Learnings based on the National Defence Industry Survey report 2018–2019 and broader economic trends are shared (pages 23–33).
 - Existing support levers available to industry seeking to develop Defence industrial capability (Annex B) (pages 38–44) and the specific actions to be taken by government to support this Priority (pages 34–36).
- 

EXECUTIVE SUMMARY

The capabilities and technologies discussed in this Advanced signal processing Industry Plan, and in the Surveillance and intelligence Industry Plan, are crucial for the ADF in an increasingly congested information domain but are complex and not readily understood in the broader community. This Industry Plan seeks to explain these capabilities, and to help businesses with relevant capabilities in adjacent sectors access opportunities to be involved.

Modern warfare is increasingly data-driven, and the ability to sense, understand and manipulate the electromagnetic spectrum is critical to warfighting advantage. A sovereign capability in advanced signal processing is therefore vital for Australia's ability to shape our strategic environment, deter any potential actions against our interests, and respond with credible military force as required. Traditional military capability has easily recognisable forms such as frigates, submarines or helicopters. Advanced signal processing capabilities represent the future of warfare, enabling us to see our adversaries, hide from them, and disrupt their critical systems and communications while protecting our own.

The industrial capabilities underpinning the integrated sensor networks and advanced signal processing technologies that enable us to identify and track our adversaries are the same capabilities that facilitate ADF activities in the electromagnetic spectrum. These are the capabilities that enable the ADF to deny, degrade, deceive or destroy adversary communications and sensors, and to counter cyberattacks on military platforms and personnel. Essential talent in software development and engineering, information technology, pure and applied mathematics, data science, and specialist engineering underpins these capabilities. Increasing Australia's capability and capacity in these key skills will help meet the ADF's needs. Also critical for this Priority is industry recognition of security requirements, including the maintenance of security clearances and the requirements associated with working with technology provided by our trusted partners.

In addition to assessing and manipulating the battlespace, military platforms must actively manage their signatures to assure their lethality and survivability in contested operating environments. As Australia continues to develop advanced signal processing capabilities, so will our potential adversaries. Digital and electronic signature management technologies that make it harder for our adversaries to find, fix, target and track our platforms will continue to be critical for the ADF. Developing these technologies requires a comprehensive understanding of advanced signal processing technologies, how platforms appear to different sensor types, and how different sensors work. Defence therefore needs an integrated approach to military platform signature management to counter the advances of potential adversaries. It is important to note this Plan is focused on digital and electronic signature management solutions, and does not include coatings or paint in its scope.

Advanced signal processing and signal management capabilities and technologies (detailed in diagrams on pages 14–15 and 17–18) are subject to a rapid rate of refresh, with a lifecycle measured in weeks or months, not years or decades like other capabilities. Agile and innovative businesses will be able to expand and grow through Defence projects, and by exporting to our alliance partners. The digital nature of these capabilities also presents opportunities to businesses in adjacent sectors such as cyber security, the space industry, commercial information and communications technology, which have the skills required to support these defence capabilities. This Plan provides direction and guidance to help foster the innovation and collaboration required to grow these capabilities locally, and to ensure that Australia stays at the forefront of rapid rate of technology refresh.

While other Sovereign Industrial Capability Priorities identified by Government tend to have a greater manufacturing focus, this priority, and the Surveillance and intelligence Priority, are supported by a digital and highly specialised industry. This industry generates firmware, software, software-defined hardware and data, with a workforce consisting predominantly of data scientists and software engineers, as well as electronic and systems engineers.

Related Sovereign Industrial Capability Priorities

Due to their shared capability building blocks and close linkages, this Plan should be read in conjunction with the *Surveillance and intelligence* Industry Plan. The *Advanced signal processing* Industry Plan is focused at the tactical level, primarily sensors and sensor integration at the platform level, including the technologies that enable the warfighter to see their adversary, remaining hidden from them, and disrupt their systems. Meanwhile, the *Surveillance and intelligence* Industry Plan is focused at the strategic level. The *Surveillance and intelligence* Industry Plan includes persistent surveillance technologies such as high frequency over-the-horizon radar and the emerging space domain, as well as force-level integration, analysis and fusion of data from tactical sensors, and the dissemination of intelligence across the Joint Force.

The Enhanced active phased array and passive radar capability Priority is also closely related to the Advanced signal processing Priority, and focuses on a single sensor technology of critical importance to Defence. Phased array radar technologies benefit from advanced signal processing capabilities, including sensor fusion with other tactical sensors at the platform level.

Advanced signal processing

This Priority is underpinned by five critical industrial capabilities. Australia seeks to have access to, or control over, certain elements of each, and to support or influence related defence industry investment. Developing these critical industrial capabilities will ensure Australia has access to world-leading advanced signal processing technologies that meet the ADF's unique requirements and extend Australia's warfighting advantage.



A DIGITALLY-CAPABLE AND SPECIALISED WORKFORCE

Industry must develop and retain a highly skilled workforce with essential talent in software development and engineering, information technology and data science, and highly advanced electronics and systems engineering.



SIGNAL PROCESSING ALGORITHMS AND SOFTWARE

Design, develop and sustain advanced signal processing algorithms and software for radar, electronic warfare, imaging and sonar sensors.



REAL-TIME DATA PROCESSING

Design, develop and sustain sensor fusion and real-time data processing, exploitation, dissemination, and presentation algorithms, and software that enhances situational awareness, threat warning and targeting.



MILITARY PLATFORM SIGNATURE MANAGEMENT

Design, develop and sustain integrated hardware and software solutions to reduce the electronic and digital signatures of military platforms to decrease the likelihood of detection and identification by an adversary's sensors.



TACTICAL SENSOR INTEGRATION

Integrate tactical sensor hardware and software with host platforms, other sensors and control systems (including combat management systems), and certify integrated sensor networks for operational use.

No single advanced signal processing or signature management technology—no matter how independently capable—is operationally effective in isolation. Defence needs industry support to successfully integrate these sensors into a holistic and comprehensive sensor network. Defence recognises these sensor networks will include best-in-breed technologies from both Australian industry and trusted foreign suppliers. Ongoing upgrades to sensor fusion, data processing algorithms, and software will enable the ADF to meet the rapidly evolving challenges associated with operating in the information domain, and electromagnetic spectrum.

A global shift towards open systems architecture will enable new advanced signal processing and signature management technologies to be rapidly adopted by the ADF and integrated into existing systems and platforms. This architecture provides flexibility as missions, threats and operating environments change, while also ensuring interoperability with our allies. Embracing this approach also provides Australian industry greater export opportunities to trusted partner militaries, as world-leading and innovative Australian technologies that can easily be incorporated in global supply chains.

In addition to the identified critical industrial capabilities listed in this Plan, the following enablers will be critical over the next decade.

- A skilled and security cleared workforce of software and systems engineers, data scientists and software developers. A focus on workforce is essential given the digital nature of this Priority. Defence is expanding existing requirements for appropriately skilled workers.
- Agility within the sector is required to continually update and upgrade the critical systems and technologies underpinning our signal processing capabilities to respond to the dynamic and evolving threat environment.
- Secure collaboration infrastructure reduces cost-of-entry barriers for businesses seeking to enter the defence market by providing shared access to accredited secure facilities and computer networks. Secure infrastructure also promotes collaboration between Defence and industry to deliver the capability solutions that ensure the ADF is cyber-ready.
- Data access for trusted Australian industry partners—particularly threat and operational intelligence data—and other technical information will facilitate capability solutions for the ADF. Data access is an essential enabler of technology development, supporting research and development by highlighting to industry the challenges faced by the ADF.

The recognition of advanced signal processing capabilities as a Sovereign Industrial Capability Priority provides industry with the certainty to invest in research, intellectual property and its skilled workforce. This Industry Plan also includes details on support mechanisms available to businesses in Annex B.

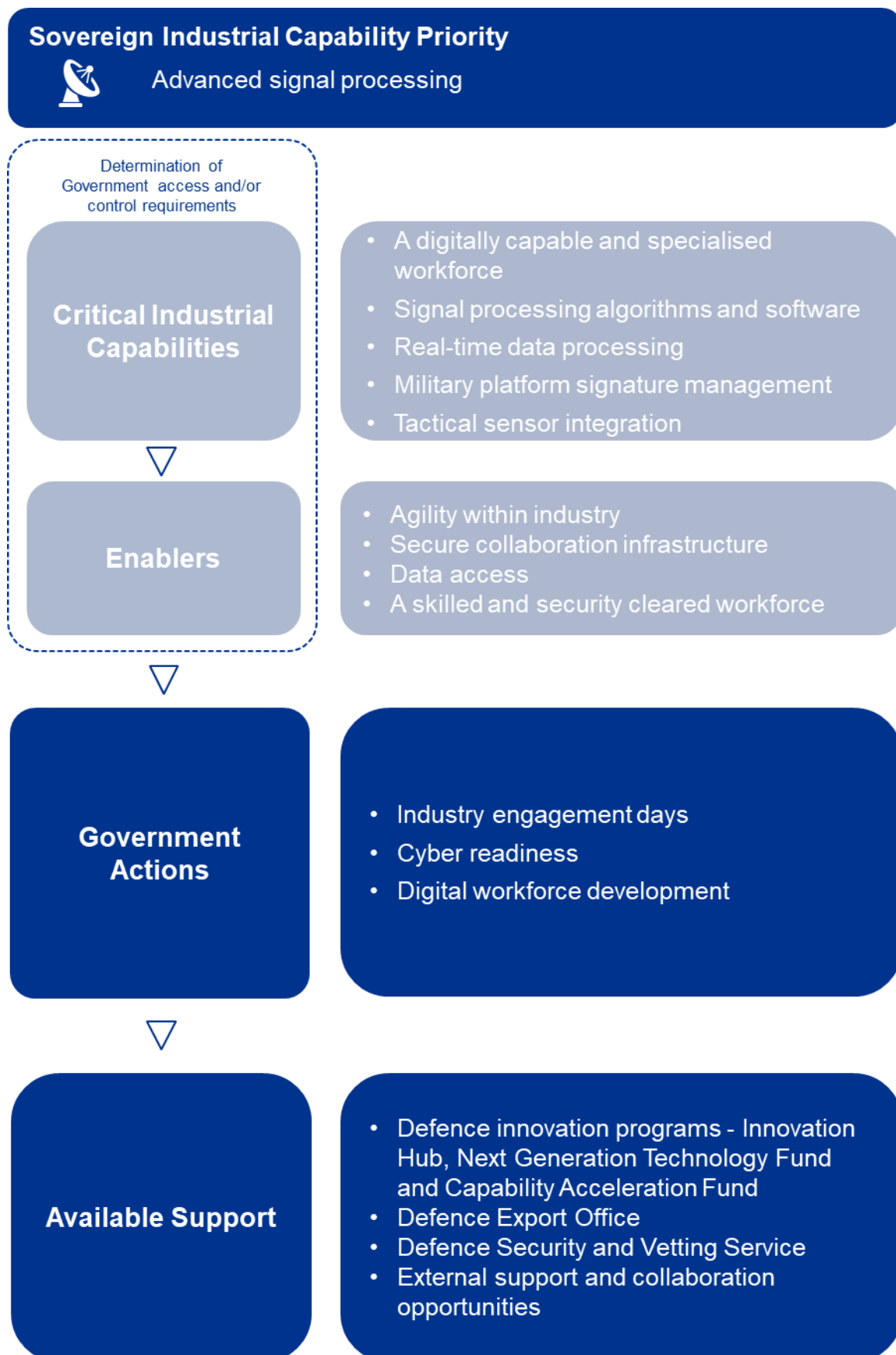
Successful implementation of this Plan

This Industry Plan describes Defence's priorities for the next three to five years in growing advanced signal processing capabilities within Australia. Successful implementation will create an industrial landscape in 2024–2026 with the following characteristics:

- Most tactical sensors on ADF ships, submarines, vehicles and aircraft will use and benefit from world-leading Australian-developed signal processing algorithms and software, even if the rest of the sensor or its host platform was acquired from a foreign supplier. These technologies will be continuously refreshed to maintain ADF warfighting advantages against rapidly evolving threats.
- Military platforms will use and benefit from Australian-developed electronic and digital signature management solutions, even if the platform was acquired from a foreign supplier.
- Australia will be a significant contributor of sensor and sensor fusion technologies to other Five Eyes partners through exports and government-to-government technology transfers. Australian-developed technologies will be compliant with open systems architecture principles and Five Eyes interoperability standards. Australia will meaningfully contribute to the ongoing evolution of those technical standards and will be recognised as an innovation leader in these technologies.
- Healthy and collaborative relationships between primes, small business, universities and Defence—including infrastructure and data sharing arrangements—will foster innovation, increase sovereign capability and create competitive advantages for Australian exports.
- Australian industry has a highly skilled workforce and is developing dual use technologies that provide Australia with a warfighting advantage, as well as benefits for adjacent sectors and the broader economy.

Features of this Sovereign Industrial Capability Priority Industry Plan

This Industry Plan describes the Advanced signal processing Sovereign Industrial Capability Priority and specific sovereign capability requirements across four key areas. These are standard across all Industry Plans and are presented below and discussed throughout the Industry Plan.



CONTENTS

SECRETARY OF DEFENCE AND CHIEF OF THE DEFENCE FORCE FOREWORD	3
EXECUTIVE SUMMARY	5
STRATEGIC CONTEXT	10
The case for a sovereign industrial base.....	10
Sovereign Industrial Capability Priority development	11
Policy framework	11
ADVANCED SIGNAL PROCESSING	12
Tactical sensor technologies.....	14
Integration, fusion and analysis of data collected by sensors	15
Signature management capabilities.....	17
Physical, electronic and digital signatures.....	18
Open systems architecture.....	18
Capability building blocks.....	19
Critical industrial capabilities	20
Global opportunities.....	21
Adjacent industries.....	21
Future evolution.....	21
CURRENT AUSTRALIAN INDUSTRIAL CAPABILITY.....	23
Australian industry attributes.....	24
Value chain	28
National capability overview	28
Workforce and technical skills.....	29
Industrial processes supporting Sovereign Industrial Capability Priority technologies.....	30
Assets and infrastructure.....	31
Australian defence industry as a global leader.....	31
Risks to domestic industry	32
BUILDING INDUSTRIAL CAPABILITY	34
Industry capability enablers	34
Building a signature management industry in Australia.....	36
ANNEX A. GOVERNMENT ACTIONS.....	37
ANNEX B. SUPPORT THROUGH INDUSTRY PROGRAMS.....	38

STRATEGIC CONTEXT

The case for a sovereign industrial base

Sovereign industrial capabilities are considered operationally critical because of the essential strategic advantage they provide to the ADF. They must be developed and supported by Australian industry because overseas sources do not provide the required security or assurances of access and supply. Australia must consider how we develop, maintain or enhance these capabilities and the degree of access to, or control over, them that we need now and in the future.

Sovereign Industrial Capability Priorities are those industrial capabilities assessed as:

- operationally critical to the Defence mission;
- priorities within the Integrated Investment Program over the next three to five years; or
- in need of dedicated monitoring, management, and support due to their industrial complexity, government priority, or requirements across multiple capability programs.¹

The initial Sovereign Industrial Capability Priorities are:



The Australian Government will make judgements about the optimal level of access to, or control over, each Priority on a case-by-case basis. A defence capability does not necessarily need to be designed, developed, manufactured, or maintained in Australia. The level of sovereign access, or control, may vary for each Priority. Defence industrial sovereignty is made up of many elements and may include:

- access to resident technical design capabilities (for example, to modify or upgrade systems);
- the ability to test and ensure that equipment is operationally ready for service or to be returned to service;
- access to, or control of, the facilities, technologies, and intellectual property underpinning our defence capability within Defence and Australian industry;
- access to allied capability that supports our warfighting advantage; and/or
- the ability to protect foreign-sourced, controlled technologies employed by the ADF.

'Access' refers to the availability of key assets within Australia able to be used by Defence if required.

'Control' is more likely to be obtained by Defence through government ownership or exclusive rights to a critical asset such as specialist machinery or infrastructure.

¹ <http://www.defence.gov.au/SPI/Industry/CapabilityPlan/Docs/SICP-Factsheet 1.pdf>

The Priorities represent only a subset of Australian defence industry capability. They identify a number of elements of the Australian defence industrial base at a capability, rather than a company or technology level. This is to encourage innovation and development in the technologies and capabilities most essential for Defence.

Sovereign Industrial Capability Priority development

These Priorities were developed through a rigorous assessment framework which considered the strategic, capability, and resource dimensions of industrial sovereignty against the needs of Defence. Consideration of industrial capabilities was balanced against Defence's priority to provide the ADF with cost-effective, cutting-edge capability that maximises Australian industry involvement.

Management and support for the Priorities starts at the very beginning of Defence planning and continues throughout the Force Design Cycle and Capability Life Cycle—including the Australian Industry Capability Program—into government grants and initiatives to support industry directly. The Australian Industrial Capability Program remains the critical lever for Australian industry involvement in supporting the Priorities and Defence's broader capability needs.

Policy framework

The *2020 Defence Strategic Update* sets out the Government's response to our changing environment. Australian industry will continue to play a major role in delivering the long terms plans for the defence of Australia and its national interests, set out in the *2016 Defence White Paper*. Industry's role as a Fundamental Input to Capability was reaffirmed in the *2020 Defence Strategic Update*, with Defence and broader government formalising the critical role defence industry plays in generating military capability and supporting the ADF.

The *2020 Defence Strategic Update* and *2016 Defence White Paper* is complemented by:

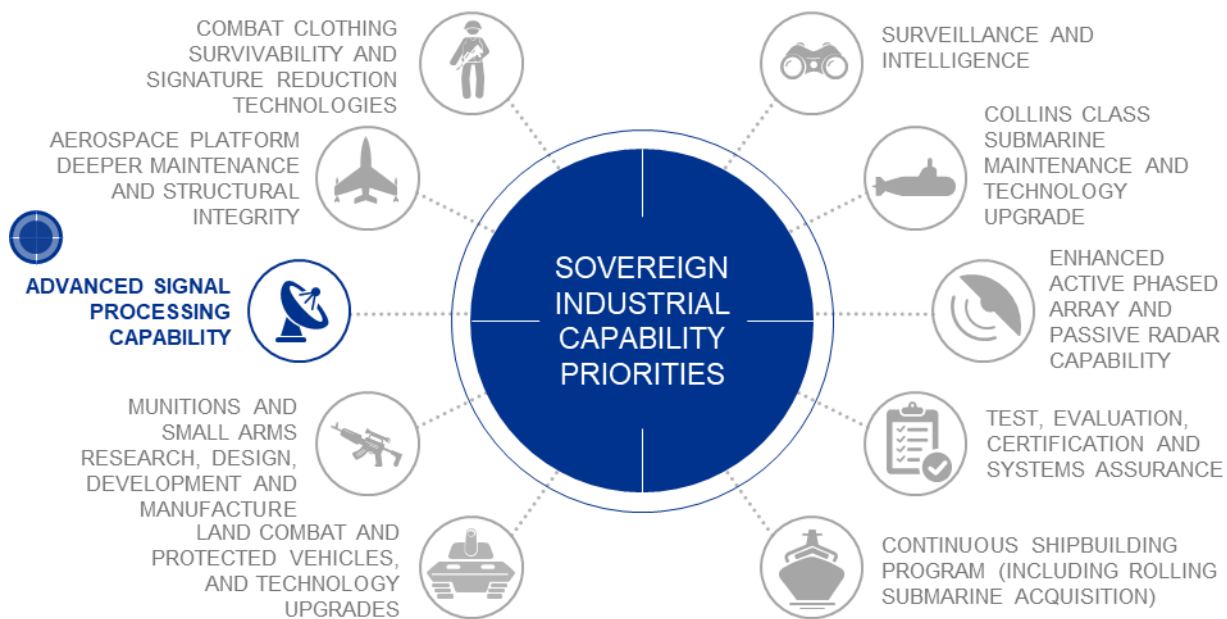
- the *2020 Force Structure Plan* and the Integrated Investment Program, which outlines \$270 billion of Defence capability investment and provides industry with the certainty to invest in people and infrastructure; and
- the *2016 Defence Industry Policy Statement*, which provides the foundation to take the partnerships between Defence and industry to new levels of cooperation, with a focus on stronger, more strategic partnerships and closer alignment between industry investment and Defence capability needs. The Defence Industry Policy Statement also provided the criteria to identify Sovereign Industrial Capability Priorities.



ADVANCED SIGNAL PROCESSING

Australian industry must understand, design, develop and use technology applications to maintain an advanced signal processing capability in the area of cyber and information security, radar, sonar and acoustic technologies, electronic warfare operational support (including threat recognition, targeting and planning), and signature management.²

Advanced signal processing and signature management technologies are critical for military platforms, and underpin our three strategic objectives of shape, deter and respond. Advanced signal processing and signature management technologies provide comprehensive real-time situational and tactical awareness, threat warning and targeting information. These technologies also make it harder for potential adversaries to identify and track Australian assets in the battlespace, and enable the ADF to operate in, and influence, the electromagnetic spectrum. These capabilities enable the ADF to disrupt the key systems of our adversaries, while protecting our own through multi-purpose sensors and transmitters.



No single sensor can provide a complete picture of the dynamic and complex modern battlespace.

Defence needs a multi-domain network of diverse and dispersed sensors across all domains with advanced signal processing capabilities to effectively observe, understand and manipulate the battlespace. Defence must deploy a number of different sensors with cutting-edge advanced signal processing capabilities that can operate effectively across all domains—including in sub-optimal conditions—and detect different types of signals.

Just as Australia develops tactical sensors with advanced signal processing capabilities, other nations will develop their own sensors that we must be able to counter. Defence needs industry assistance to develop an integrated approach to military platform signature management to keep our platforms hidden in the electromagnetic spectrum. As our strategic environment becomes increasingly congested and complex, and with Australia's interests being more directly challenged, signature management capabilities will become increasingly vital for the ADF.

² Defence Industrial Capability Plan 2018.

Tactical and strategic capabilities

Sensors actively or passively measure electromagnetic waves above water, acoustic waves below water, or network traffic in cyberspace. Advanced signal processing capabilities enable these sensors to gather data from different environments—and transfer and present that data in a meaningful way—at both the tactical and strategic level:

This Plan characterises tactical and strategic in the following ways:

- tactical refers to input from a single sensor, or system of sensors on a single platform, that informs the warfighter of their immediate battlespace
- strategic refers to input from multiple sensors and systems across the Joint Force, including land and space-based capabilities, that provide a holistic overview of the broader battlespace.

This Plan focuses on information gathering and assessment at the tactical level, including individual sensors embedded within a platform. This Plan also includes the fusion, analysis and assessment of data from multiple sensors within a platform, but not the integration with the broader Joint Force. Military platforms and personnel are often operating in remote and degraded environments, and not always able to rely on information and intelligence from broader strategic capabilities.

Data from multiple sensors and platforms, including fixed installations such as the Jindalee Operational Radar Network, are also processed at the strategic level by surveillance and intelligence capabilities. This information is fused, analysed and disseminated as intelligence across the Joint Force to support broader situational awareness, threat warning and targeting. These strategic capabilities are detailed in the Surveillance and Intelligence Industry Plan.

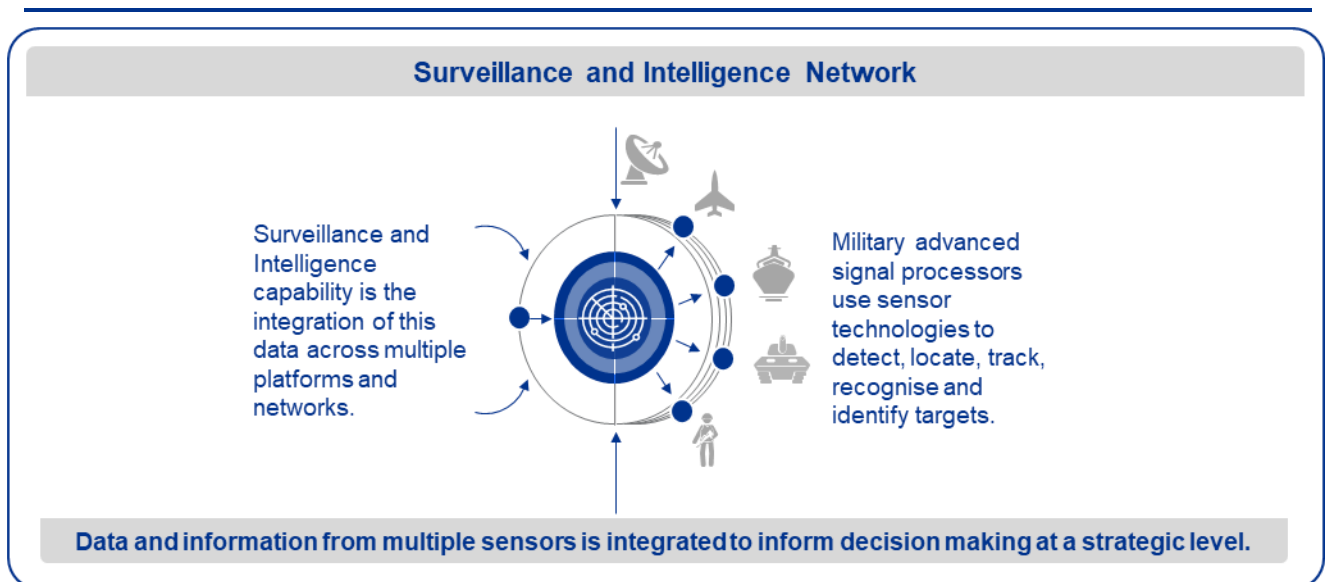


Figure 1: Surveillance and intelligence network

The digital industry

This Priority is supported by a digital industry with underpinning capabilities based primarily on firmware, software, software-defined hardware, and data. Australia has world-leading skills and capabilities in this area and can provide locally sourced solutions where access to the required technology is not available through trusted international primes.

This workforce predominantly comprises data scientists and software engineers. The critical enabling infrastructure is information and communications technologies. It is imperative that this skilled workforce is grown and maintained in Australia. A skilled workforce is crucial to harnessing these digital capabilities and ensuring Australian industry has the agility to meet challenges associated with the modern battlespace and an evolving security environment.

This industry Plan is closely related to two other Priorities:

Surveillance and intelligence

The Surveillance and intelligence Industry Plan addresses the enterprise-wide integration of sensor data and intelligence in national command, control, communications, computing and intelligence systems. It also addresses national persistent surveillance capabilities such as high frequency over-the-horizon radar, space domain awareness, and space-based surveillance systems.

The capabilities outlined in the *Advanced signal processing* Industry Plan underpin the modern communications systems and networks captured in the *Surveillance and intelligence* Industry Plan, and facilitate secure communications across the Joint Force.

Enhanced active array radar and passive radar

The Enhanced active phased array and passive radar Industry Plan focuses on a radar sensor technology of critical importance to Defence, in which Australian industry has a world-leading capability. The Plan encompasses advanced next generation multi-function radars and passive radars that leverage third-party transmissions to detect and track targets. Modern radars are elements of a broader, networked warfare capability, and benefit from advanced signal processing capabilities, including sensor fusion with other tactical sensors.

Advanced signal processing capabilities and technologies are of particular importance for active phased array radar technologies as they provide protection from electronic attack and enable target identification in a congested and contested electromagnetic spectrum.

Defence relies on Australian industry to support its signal processing and signature management capabilities, and to maintain operational effectiveness against rapidly evolving threats. To ensure Defence's needs are met, industry must remain flexible and agile, with the ability to pivot to different solutions as the security environment and the abilities of our potential adversaries evolve.

Government is committed to broadening and deepening the industrial base that supports this Priority. However, new entrants to the sector must be aware that applicable technologies are often highly classified, and exports are often restricted to Five Eyes partner nations. Australian industry providers must therefore maintain suitable security credentials to ensure continued access to Five Eyes interoperability standards. This will:

- meet Defence security requirements
- allow Australian industry to take advantage of export opportunities to other Five Eyes nations
- help industry to embed itself in global supply chains.

Tactical sensor technologies

Tactical sensors use digital signal processing to convert analogue measurements of objects and the environment into data. This data can then be processed and exploited to support situational awareness, threat warning and targeting. Most military platforms use one or more types of tactical sensors to observe their operating environment and objects of interest, such as other military platforms, personnel and key terrain features.

Military sensor technologies are primarily designed to detect, locate, track, recognise and identify targets in all domains in the battlespace. However many of these sensor technologies are becoming increasingly multi-purpose and can also be used to manipulate, shape and influence the electromagnetic spectrum.



Active radar

Radar transmits directed radio waves into the atmosphere at specific frequencies, and listens for reflected energy from objects of military interest such as aircraft and ships. Radar is highly effective at detecting, locating and tracking targets with high precision at long ranges in all weather conditions and environments above water. The active transmission of radio waves by a radar can reveal its position and make it vulnerable to attack.



Passive radar

A specialised type of radar that does not transmit its own radio waves, but detects, locates and tracks targets by leveraging third party transmissions. Passive radar does not reveal its position but depends on transmissions from other sources (such as television and radio broadcast towers) to be present in the battlespace.



Electronic warfare

Electronic warfare can manipulate the electromagnetic spectrum to provide warfighting advantages for the ADF. In the context of advanced signals processing, electronic warfare sensors listen for radio waves transmitted by radars and radio communication systems. Electronic warfare sensors are highly effective at detecting targets at long ranges in all weather conditions and environments, except underwater, and also for recognising and identifying targets. It is less effective for locating and tracking targets, unless multiple dispersed sensors are networked. However, they are only effective against targets that can be exploited through the electromagnetic spectrum.



Imaging sensors

Imaging sensors measure the radiation emitted by targets and the environment in the visible band, infrared band or other wavelengths to generate still images or videos. Imaging is effective at detecting and locating targets, and highly effective at tracking, recognising and identifying targets, but does not work in all weather conditions. Imaging sensors are passive and do not reveal their position by actively transmitting.



Synthetic aperture radar

A specialised type of radar that transmits radio waves for long periods of time and integrates reflected energy to synthesise images. Synthetic aperture radar has similar characteristics to imaging sensors, with the added advantage of all-weather capability, but its active transmission of radio waves makes it vulnerable to attack.



Acoustic (Sonar)

Used extensively in underwater environments where other sensor types are ineffective, active sonar has similar characteristics to active radar, as it transmits pulses of acoustic energy, and listens for echoes. Passive sonar listens for sounds emitted by targets and has similar characteristics to passive radar and electronic warfare sensors.



Seismic sensors

Seismic sensors are used to detect ground movement, based on sound and soil vibrations. These sensors have the ability to categorise ground movements by detecting and classifying unique seismic signatures. Seismic systems are typically used to detect land based platforms and other ground based military activities.

Each sensor type has advantages and disadvantages, and the integration of a diverse range of sensors across all domains provides better tactical and strategic situational awareness, threat warning and targeting than any single sensor. Defence is therefore investing in diverse sensor and sensor fusion technologies to properly harness the full potential of tactical sensors.

Integration, fusion and analysis of data collected by sensors

There is no universal sensor that is effective against all targets and in all operating environments. No single sensor—no matter how capable its signal processing techniques—is effective in isolation.

Tactical and strategic sensor integration, sensor fusion, and real-time data processing and exploitation are essential to achieving information superiority in an increasingly complex modern battlespace. As data volumes grow exponentially, sophisticated presentation and interaction techniques are becoming increasingly necessary to optimise the tactical user experience, and to allow warfighters to have the information needed to support rapid decision making. Adding to this degree of complexity is that any information exploited from sensor data must be disseminated and presented throughout the networked Joint Force to facilitate broader situational awareness.

While Australia does have high-end surveillance and intelligence capabilities, the ADF often operates in remote and degraded environments without access to the full suite of strategic capabilities. ADF personnel therefore rely on a smaller range of tactical

sensors on an individual platform. In these situations, it is critical that the ADF has the ability to collect, fuse and process data rapidly.

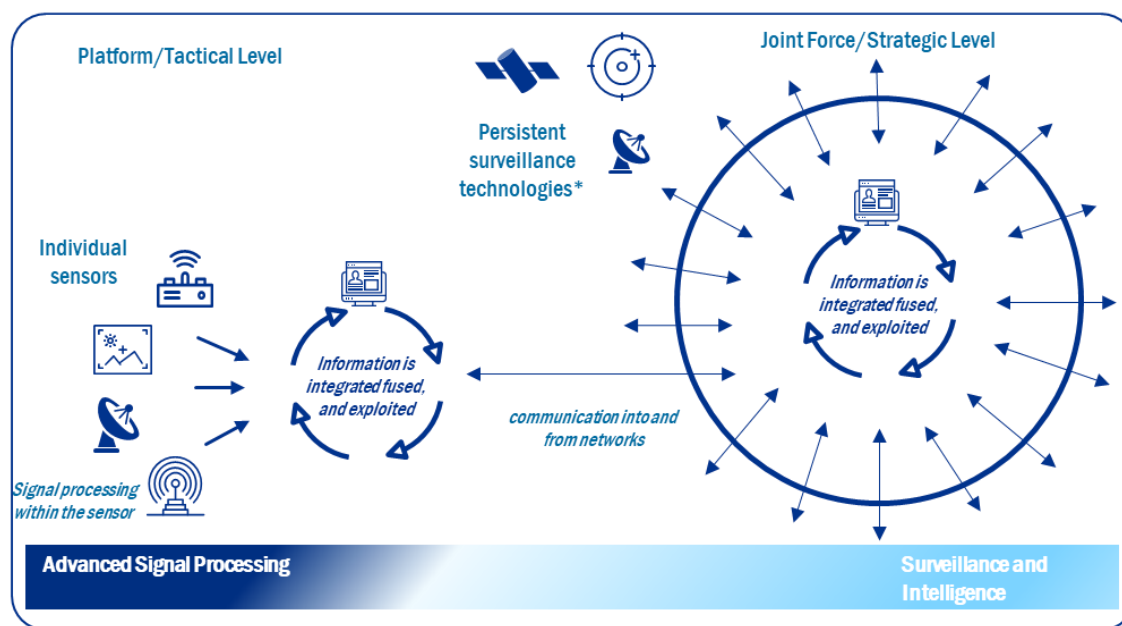


Figure 2: Interaction between the Advanced signal processing and Surveillance and intelligence Priorities

*Defence recognises there is a common set of industrial capabilities employed in both tactical sensors and in persistent surveillance technologies. However, persistent surveillance technologies are within the scope of the *Surveillance and intelligence* Industry Plan. More information on the common industrial capabilities between the two priorities is explored in the Current Australian Industrial Capability section of this Plan.

Most tactical sensors are integrated with a military platform that powers, protects and manoeuvres the sensor through the battlespace. The extent of host platform integration varies from hardware-only integration – where the sensor operates independently from other systems on the platform – through to full-hardware and software integration – where the sensor interacts with all other sensors and control systems onboard the platform. These sensors also need to be integrated with broader strategic and joint force capabilities. This broader integration is discussed in the *Surveillance and intelligence* Industry Plan.

Sensor fusion combines data from multiple sensors to produce more accurate information that any single sensor can provide. Sensor fusion is undertaken at the tactical and strategic level, and can be performed with multiple sensors of the same or different types. At the tactical level, data from sensors on-board a platform is combined and manipulated to provide real time information to ADF personnel to help make rapid decisions. At the strategic level, data across the Joint Force is collected, processed and disseminated to enhance broader situational awareness. This strategic level fusion is discussed in the *Surveillance and intelligence* Industry Plan.

Real-time data processing and exploitation are the closely related activities of preparing data for analysis, then analysing that data. Sensor technology outputs must be processed into standardised, open and non-proprietary data formats that can provide useful information to the warfighter. The value and relevance of information varies between different consumers, so matching the right information to the right consumer, and presenting it the right way—all in a timely manner—is a significant challenge.

Sensor integration in action

In an air and missile defence scenario, passive radar can be used to first detect and locate an approaching target at long range, and then to provide information to imaging sensors that can passively track the target. Electronic warfare sensors can then be used concurrently to recognise and identify the target, so an informed decision on a potential response can be made.

If it is necessary to engage the target, then active radar can be used to refine target tracking to a level suitable for precision weapons deployment. Delaying the use of active radar until late in the engagement timeline increases the likelihood that the target will be caught by surprise, unable to employ its countermeasures, and be efficiently defeated.

Signature management capabilities

A sensor's performance depends on the physical, electronic and digital signatures of its targets. A military platform with a large signature is generally easier to detect, locate and track against environmental background noise, while a platform with a distinctive signature is generally easier to recognise and identify.

Signature management disguises or distorts a platform's unique signature. This reduces the probability of detection, identification and targeting, and helps to increase operational effectiveness and platform survivability. For example, a platform can reduce or alter its signature by using materials that absorb, dissipate or scatter acoustic energy so that its unique signature goes undetected. Signature management can also include other deception techniques, such as duplicating the platform signature, creating stronger signatures in different locations, or changing the platform's signature. These are all done with advanced signal processing capabilities through digital radio frequency memory, or other software defined systems.

As this Priority is supported by the digital industry, this Plan focuses on software-defined digital and electronic signature management technologies, rather than physical signature management solutions such as paints or coatings.



Visual signature

The physical appearance of a platform as seen by the human eye, or an electro-optic imaging sensor. A platform can reduce or alter its visual signature using camouflage and concealment.



Acoustic signature

The sounds made by a platform, as heard by the human ear or a passive acoustic sensor. The specific sounds made by jet engines, helicopter rotor blades, and aircraft, ship or submarine propellers can make a platform recognisable or identifiable to acoustic sensors. A platform can reduce or alter its acoustic signature using noise-reduction techniques, sound-dampening materials and sound-scattering shapes.



Radar cross section

A measure of how large a platform appears to radar. A platform can reduce or alter its radar cross-section by using materials that absorb or dissipate radio waves, or shapes that scatter radio waves away from radar.



Sonar cross section

The acoustic equivalent of radar cross-section, and a measure of how large a platform appears to a sonar. A platform can reduce or alter its acoustic size by using materials that absorb or dissipate acoustic energy, shapes that scatter acoustic energy away from a sonar, and active countermeasures that interfere with sonar signal processing.



Radio frequency emissions

The radio waves emitted by a platform or force package's radars and radio communications systems can reveal it to electronic warfare sensors. A platform can reduce or alter its radio frequency emissions by avoiding unnecessary transmissions, transmitting at lower-power levels, using directional antennas, or using complex waveforms that overwhelm electronic warfare sensors.



Infrared emissions

The infrared energy emitted by a platform's engine exhausts, jet or rocket plumes, high-power transmission antennas, and other heat sources can reveal a platform to infrared imaging sensors. A platform or force package can reduce or alter its infrared emissions by cooling or masking its hottest parts, or diffusing its jet or rocket plumes.



Ultraviolet emissions

Jet and rocket plumes can emit ultraviolet energy at a sufficiently high level to be distinguished from the background radiation of the sun, and reveal a platform to ultraviolet imaging sensors. Reducing or altering these ultraviolet emissions is very difficult, and typically involves varying the chemical composition of the jet or rocket fuel.



Cyber signature

This is a device's digital fingerprint that appears on a network, and can include its typical data send and receive patterns, its interactions with other devices, and any unique data or metadata sent by the device. A device may be recognised or identified by a network monitoring system from its cyber signature and a particular combination of devices may be recognisable or identifiable as a military platform. Reducing or altering cyber signatures is very difficult, and typically requires frequent variations of connectivity and behaviours to break the association between digital identifiers and the corresponding platform.



Magnetic signature

Ships and submarines are mainly constructed of steel, which disturbs the earth's magnetic field. This enables vessels to be detected and identified by sensors designed to detect these disturbances. Treatments can be applied to platforms to minimise or alter their magnetic signature, minimising their vulnerability to mines and magnetic detection.

Our potential adversaries may also develop integrated networks of diverse sensors with advanced signal processing capabilities. An integrated and innovative approach to managing all aspects of military platform signature is therefore essential to counter an adversary's integrated sensor networks that apply sensor fusion techniques. To ensure the ADF can meet the changes of the dynamic and evolving battlespace, Defence is investing in and encouraging Australian industry to support sovereign capability in signature management.

A balanced approach to signature management is required

Many modern militaries have invested heavily in radar cross-section reduction for combat aircraft to reduce their vulnerability to engagement by radar-based air defence systems. Low-observability ('stealth') aircraft may be physically large but appear so small to active radar that even if they are detected, they may not be recognised as a target.

Now consider if a radar was integrated with an electronic warfare sensor and the aircraft was transmitting recognisable radio frequency energy from its radio communications systems. The integrated sensors would recognise the small radar contact as a hostile military aircraft and could initiate a threat response.

Unbalanced investment in radar cross-section reduction alone—or any other single aspect of signature management—is of little benefit to a military platform against an adversary capable of sensor fusion or other advanced signal processing. Defence will seek a balanced and agile approach to signature management wherever possible, including reducing all of a platform's physical, electronic and digital signatures.

Physical, electronic and digital signatures

Physical signature management techniques are typically built in to a military platform and must be applied very early in the value chain, such as designing structures to have an inherently small radar cross section. There is limited opportunity for Australian industry to participate in the design and development of physical signature management solutions for military platforms manufactured offshore, so these solutions are not in scope for this Priority.

Electronic and digital signature management techniques are typically software-defined and may be added to a military platform later, such as radio emissions monitoring and control systems. A military platform's electronic and digital signatures are also likely to change far more often than its physical signatures, since changes to sensors, effectors, communications systems, and many other mission systems can affect these signatures. Electronic and digital signature management capabilities require continuous technology refresh to enable Defence to adapt to rapidly evolving threats and changes in sensor capabilities. Australian industry therefore must be able to rapidly develop agile signature management solutions, ensuring that capability can remain both fit-for-purpose and effective against potential adversaries.

Open systems architecture

The United States Department of Defense is leading a shift towards open systems architecture between Five Eyes partners. Key characteristics of open system architecture include:

Modularity

Components can be removed, replaced and changed without adversely affecting an overall system.

Openness

Suppliers are willing to publish the physical, electronic and digital interface specifications of their components.

Standardisation	Interoperability
Interface requirements (including data formats and physical interconnections) are controlled by publishing common guidelines for all suppliers and monitoring compliance.	Components designed and developed by different suppliers can work together without adaptation or compromise.

There are three benefits to open systems architecture. First, it enables new technology to be rapidly inserted into military systems so those systems can adapt to changing missions, threats and operating environments. Interoperable systems built from modular components can be quickly and easily introduced into military service.

Second, open systems architecture helps promote innovation through competition by breaking vendor lock, and can also improve supply chain resilience through enabling second sourcing. Adaptation to this new commercial approach will take time and present challenges, and Defence recognises Australian industry will play a key role in this endeavour.

Third, Defence expects the open systems architecture approach to be beneficial to Australian businesses that embrace a continuous innovation business model. This is especially the case for small businesses with relevant skills that may have previously been locked out of global supply chains based on proprietary technologies.

Integrated advanced signal processing capabilities are sensitive and often attract high levels of security classification. Capabilities built using open systems architecture principles may comprise many unclassified modules that only become classified once integrated into a larger system. Algorithms and software may also be developed by industry at the unclassified level, and only become classified once they are combined with sensitive Defence data. It is vital therefore that industry protects and secures its intellectual property, products and capabilities through appropriate physical, personnel, and electronic security measures. Any loss of intellectual property could result in Australia losing a capability edge in this increasingly critical space.

Capability building blocks

Technology alone does not constitute a capability. Sensor technology must be integrated into military platforms and networked across multiple platforms in the Joint Force. Assurance of all technology components and their certification for ADF operational employment are critical for turning technology into capability.

Advanced signal processing and signature management share a common set of fundamental capability building blocks:

- systems integration
- technology, including algorithms, software and hardware components
- assurance and certification.

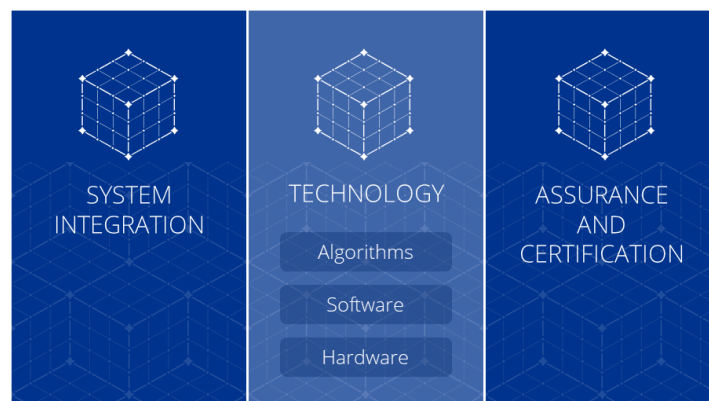


Figure 3: Capability building blocks

These building blocks apply to all stages of the value chain, and enable Australian and foreign technologies from multiple vendors to be integrated into a diverse, but cohesive, ADF sensor network. While systems integration and assurance, and certification activities are predominantly performed during the later stages of the value chain, they are also essential for design and manufacture considerations during the inception of a new capability.

While systems integration is critical to this Priority, assurance and certification is not a focus area in this Plan as it is covered extensively in the Test, evaluation, certification and systems assurance Industry Plan.

Critical industrial capabilities

Critical industrial capabilities are the industrial capabilities that underpin the Sovereign Industrial Capability Priorities. They are specific industrial capabilities that Australia seeks a level of access to, or control over. They could be an essential skill, technology, intellectual property, financial resource, infrastructure or some other industrial element. It is these capabilities that we need to protect, to ensure the ADF can deliver a capability advantage, no matter the threat.

When considering this Priority, five critical industrial capabilities have been identified. These capabilities underpin the ability to integrate current, emerging, and disruptive technologies into ADF sensors and combat management systems.



A DIGITALLY-CAPABLE AND SPECIALISED WORKFORCE

Industry must develop and retain a highly skilled workforce with essential talent in software development, engineering, information technology and data science, and highly advanced electronics and systems engineering.

Platforms, systems, and technologies that deliver advanced signal processing capabilities will continue to be replaced and upgraded. Unlike traditional military platforms that have lifecycles measured in decades—such as naval vessels, helicopters or land combat vehicles—advanced signal processing capabilities are constantly evolving. Australian industry needs a highly skilled workforce capable of upgrading and enhancing the performance of ADF tactical sensor technologies, implementing sensor fusion and real-time data processing techniques, and developing signature management technologies.

Advanced signal processing and signature management technologies are highly complex digital capabilities. They are increasingly focused on software, but still require a thorough understanding of the enabling hardware. To deliver all of the other critical industrial capabilities listed in this Plan, Australian industry needs a workforce with skills and capabilities in software development and engineering, information technology, data science and systems, electronics, microelectronics and communications engineering.



SIGNAL PROCESSING ALGORITHMS AND SOFTWARE

Design, develop, upgrade and update advanced digital signal processing algorithms and software for radar, electronic warfare, imaging and sonar sensors.

The rapid pace of threat evolution means that a continuous technology refresh is required to maintain a warfighting advantage. Australian industry needs to be agile, able to respond on short notice, with quick turnaround times, and with capabilities across a wide range of sensors and sensor technologies. This means a broad industry base is required to support all the diverse sensors employed by the ADF.

Australian industry needs to upgrade and enhance the performance of ADF tactical sensor technologies, especially for operations in contested environments against adversaries employing integrated signature management techniques. To achieve this objective we must develop innovative digital signal processing algorithms and software for radar, electronic warfare, imaging, and sonar systems and have a comprehensive understanding of the enabling hardware. Australian industry must develop sensor technologies and systems, and modify and sustain these, including individual sensors acquired from our allies to meet our unique requirements. In addition to the skills and capabilities listed above, this critical industrial capability requires skills and expertise in radio frequency engineering and propagation techniques, as well as capabilities in pure and applied mathematics.



REAL-TIME DATA PROCESSING

Design, develop and sustain sensor fusion and real-time data processing, exploitation, dissemination and presentation algorithms, and software that enhances situational awareness, threat warning and targeting.

Sensor fusion, real-time data processing and exploitation are essential to achieving superior information in the complex modern battlespace. Information exploited from on-board sensor data must be rapidly and reliably provided to enhance situational awareness, threat warning and targeting. As data volumes grow exponentially, sophisticated presentation and interaction techniques are increasingly necessary to improve the ADF experience.

Australian industry must implement sensor fusion and real-time data processing techniques for a wide range of sensor technologies at the tactical level. This will be done primarily through software development capabilities creating advanced algorithms and software that can transform, manipulate and extract valuable information from individual sensors.



MILITARY PLATFORM SIGNATURE MANAGEMENT

Design, develop and sustain integrated hardware and software solutions to reduce the electronic and digital signatures of military platforms, and decrease the likelihood of detection and identification by an adversary's sensors.

Digital and electronic signature management technologies are essential to hide platforms in the electromagnetic spectrum. Our adversaries are continually investing in sensors and technologies to find our platforms, so continual signature management solutions are required. Sovereignty in digital and electronic signature management is essential given the highly classified nature of military platform signatures.

Australian industry needs to enhance the lethality and survivability of military platforms through integrated electronic and digital signature management solutions that exceed the sensing capabilities of our potential adversaries. These solutions will be achieved through industrial capabilities in digital signal processing and real-time data processing. These capabilities can measure and characterise the signatures of military platforms and, by applying signature reduction capabilities, change the signatures of military platforms. As this priority is focused on digital and electronic signature management, industry will require significant software development modelling capabilities and engineering.



TACTICAL SENSOR INTEGRATION

Integrate tactical sensor hardware and software with host platforms, other sensors and control systems (including combat management systems), and certify integrated sensor networks for operational use.

Success in modern military operations depends on providing the ADF with comprehensive real-time situational awareness, threat warning, and targeting information. No single sensor type operating in any single domain can provide a complete picture of the dynamic and complex modern battlespace. Defence platforms therefore need a multi-domain network of diverse and dispersed sensors to effectively observe and understand the battlespace. This network must integrate sensors from key partners into ADF platforms.

Australian industry needs complex systems engineering and integration capabilities to integrate tactical sensor technologies with host platforms, other sensors and control systems (including combat management systems) on military platforms. Integrating Australian and Five Eyes technologies and capabilities is essential to satisfy the unique operational requirements of the ADF, as well as the environmental characteristics of our region. Networking different sensor technologies on military platforms will also be required to support networked sensor fusion and real-time data processing.

Global opportunities

Advanced signal processing technologies represent export opportunities for Australian industry, where innovations in sensor, sensor fusion and real-time data processing technologies can be exported to other Five Eyes nations. Defence expects Australian industry to adopt and contribute to the emerging body of Five Eyes technical standards for sensor interoperability, both to support the ADF and to ensure their continued access to export markets. Investing and developing these critical industrial capabilities increases sovereign capability and enables global opportunities for Australian industry.

Adjacent industries

The Advanced signal processing Priority provides opportunities for businesses in adjacent industries, such as cyber security, the space industry, and information and communications technology. Businesses in these sectors with critical industrial capabilities could contribute to the defence industry sector. However, businesses moving in to the sector must ensure they meet security requirements, and have an appropriately cleared workforce.

Future evolution

The world is full of innovative commercial technologies that could have valuable military applications or be disruptive to established military capabilities. Most of these technologies are software-defined and will progress through multiple generations in the time it takes Defence to responsibly acquire and safely field a new ship, submarine, combat vehicle or aircraft. Defence acquisition and sustainment practices are evolving to support rapid technology insertion, and Defence needs Australian industry to be attuned, agile and prepared to respond to emerging and disruptive technologies and threats.

Advanced signal processing

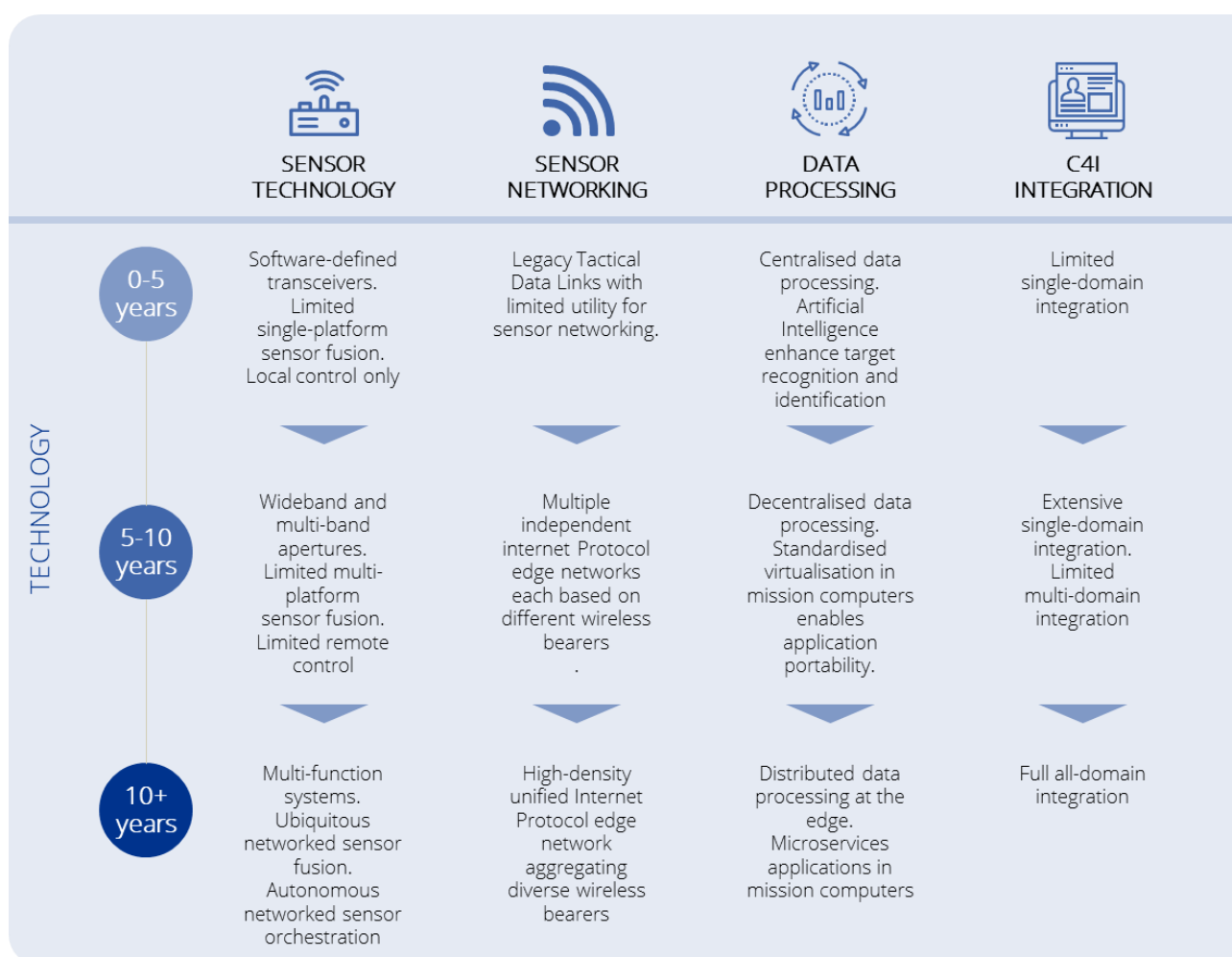
The next significant evolution in advanced signal processing will be ubiquitous networked sensor fusion. The ADF already operates niche sensor fusion capabilities on some of its high-end combat platforms, such as the F-35A Joint Strike Fighter and Hobart-class Air Warfare Destroyer. In these platforms, multiple sensors are aggregated and sensor data can be fused locally, or between multiple platforms of the same type using special-purpose networks. Emerging digital signal processing, wireless communications, data networking and distributed computing technologies can enable a diverse range of sensors to be fused using general-purpose networks.

This networked sensor fusion allows the ADF to disaggregate its sensors amongst multiple platforms operating across all domains, for greater tactical survivability and operational flexibility. Defence also expects greater use of artificial intelligence techniques within sensor fusion over the next decade.

Signature management

The next significant advancement in signature management is dynamically adaptive signature management enabled through artificial intelligence techniques. Adaptive signature management will be critical to maintain ADF warfighting advantages against potential adversaries that may introduce artificial intelligence to their sensor fusion capabilities over the next decade. Defence is attuned to digital twin technologies and other high-fidelity modelling and simulation techniques, particularly their use in more integrated approaches to military platform signature management.

The following graphic summarises key technology trends in sensor technology, sensor networking, data processing, and command, control, communications, computing and intelligence (C4I) system integration. These trends will influence this Sovereign Industrial Capability Priority and the closely related Surveillance and intelligence Priority over the next decade.



CURRENT AUSTRALIAN INDUSTRIAL CAPABILITY

The Advanced signal processing and Surveillance and intelligence Priorities are served by a highly skilled Australian defence industry sector. While each of these priorities links to different but closely related areas of Defence capability, both priorities share the same industrial base.

This sector is a digital industry focused on technology that is continuously and rapidly evolving, so businesses must be agile and innovative to keep pace. Australia has a diverse and growing industrial sector supporting advanced signal processing, and surveillance and intelligence capabilities. Australian industry possesses world-leading research and development of signal processing for imaging, sonar and passive radar. We have an opportunity to grow a signature management capability in Australia that will enable home-grown solutions to meet the unique requirements of the ADF. Organisations in this sector vary in size from micro-businesses to large international primes, and their approach to research, development and delivery of products and services also varies greatly.

The Defence value chain outlines on page 28 the activities involved in the research and development, design, manufacture, integration, and modification stages of the capabilities critical to this Priority. Enablers and inputs to each activity are assessed for their relative impacts with a view to understanding the strengths and weaknesses of the domestic industry, as well as to determine if action needs to be taken to ensure that Defence has the access, or control, it needs in relation to this Priority.

Manufacturing advanced electronic components in Australia is unlikely to become economically viable in the foreseeable future, and hardware manufacturing is not a prerequisite or requirement for this Priority. What is important is the capability to develop software and algorithms in Australia, and understanding the design of individual components. Access to intellectual property is critical, and must be managed by a highly educated and technically skilled workforce. Security is a critical consideration throughout the value chain, given the value and sensitivity of both advanced signal processing and surveillance and intelligence capabilities.

This chapter describes the common industrial base that services both the Advanced signal processing and Surveillance and intelligence Priorities. Attributes and features that are unique to the Advanced signal processing are highlighted with the following symbol:



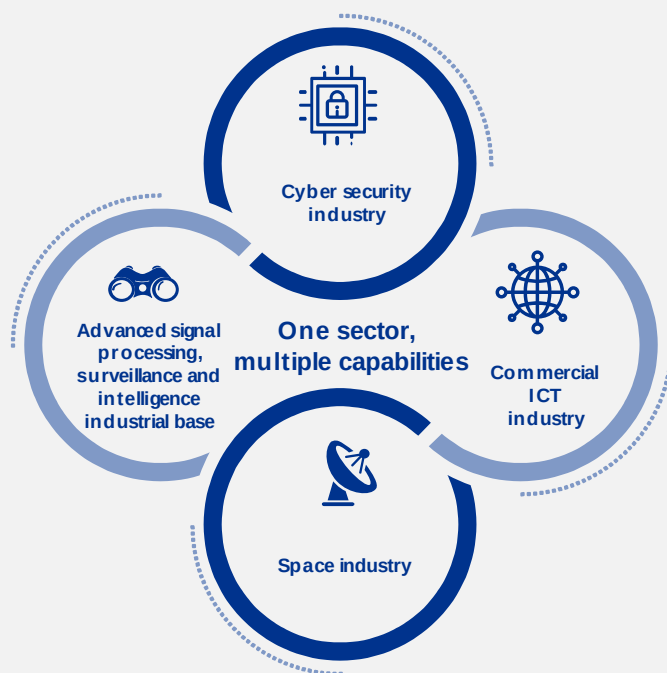
Australian industry attributes

Insights into the attributes of current Australian industry capability are the result of findings from extensive consultation undertaken during the development of this Plan. Research and analysis into the composition and characteristics of Australia's industrial base was also undertaken through a Centre for Defence Industry Capability survey. The breakdown of Australia's industry in this section is based on data gathered during industry consultations across all Plans, covering 141 organisations, and the Centre for Defence Industry Capability survey.

One sector, multiple capabilities

The Advanced signal processing and Surveillance and intelligence Priorities are supported by a shared industrial base. While individual Defence requirements can differ across the two Priorities, there are a number of common industry capabilities that service both, leveraging the same key skills, assets and infrastructure. This industrial base also intersects with other Australian industries including commercial ICT, cyber security and space.

This overlap and commonality among the industries brings both strengths and challenges. The knowledge and capability in commercial industries can be leveraged to advance the defence industry, but also brings significant competition when it comes to hiring and retaining the right people. There are other major customers internationally and within the Australian Government that are competing for the same resources as Defence. In particular, the commercial ICT, cyber security and space industries all have a healthy pipeline of work, and through consultations, many organisations in defence industry noted they are also servicing national security clients.



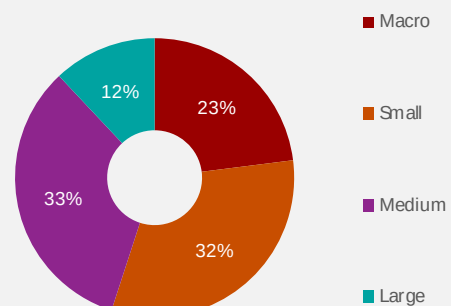
Size and composition

The majority of respondents to the survey who indicated an ability to support this Priority are small and medium businesses³ representing 65 per cent of the industry sample.

The data used in this section reflects information collected and provided by the Centre of Defence Industry Capability.⁴ While the collection process for this data is subject to respondent interpretation, it provides an industry snapshot of contributors to value chain activities. The insights gained from extensive industry consultation undertaken during the development of this Plan—as well as in-depth research and analysis—provides a deeper understanding of the composition and characteristics of Australia's industrial base and current Australian industry capability.

Due to the niche nature of these capabilities, the Australian Bureau of Statistics census data does not provide sufficient granularity or specificity for this industry, and could not be used for this Plan.

Business Size (Pie)
of respondents = 382



Note: Percentage of respondents of a specified business size, based on the number of employees in Australia

³ The survey categorises organisations as micro (up to four employees), small (five to 19 employees), medium (20 – 200 employees) and large (200+ employees).

⁴ The survey, administered by the Centre for Defence Industry Capability in 2018 required industry to complete a range of questions in relation to their business and the industrial capabilities able to be generated with a Defence application. Approximately 1,800 organisations responded to this survey and the data collected was self-reported, and not validated through other sources; accordingly there are limitations in terms of data bias and representation of the sector.

A digital workforce

As a digital industry, this sector is different to others in defence industry, which tend to have a greater focus on manufacturing. The sector supporting this priority relies on a highly educated digital workforce of software developers and engineers, information technology professionals, data scientists, and specialist engineers in disciplines such as radio frequency, optics and photonics, and digital signal processing. These data scientists and specialist engineers often require PhD qualifications to progress beyond entry level in this sector, and once highly specialised cannot readily switch roles. For example, a radio frequency engineer specialising in radar would require years of training to become an electronic warfare expert. Businesses in this sector must also compete with global technology companies to recruit the limited number of graduates from Australian universities, and that is only the beginning of a long investment in talent development.

However, while the foundational education needed by this workforce is common with commercial digital industries, Defence has many unique requirements such as Australian citizenship, security clearances, expertise in military specific technologies, and an understanding of Defence business processes and military operating concepts. Businesses in this sector cannot simply tap into the highly commoditised generic information technology workforce to work on Defence projects; they must invest significantly in upskilling graduates and transitioning lateral recruits from other industries. These businesses also face the continual risk of losing their skilled, cleared workforce to the commercial digital industry that can often offer higher rates of remuneration.

While commercial technologies are often adaptable to Defence needs, Defence must protect sensitive and valuable advanced signal processing, and surveillance and intelligence technologies, to maintain ADF warfighting advantages. Being unable to publicly disclose their technological achievements can be commercially challenging to businesses in this sector, especially when competing with global technology companies for a limited digital workforce. Increased industrial investment from industry in the critical capabilities that underpin this Priority will deliver benefits to the broader economy, as greater capability in data science and software engineering will help place Australia at the forefront of the global technological revolution, and lead to innovation in other sectors of the economy.

Sustaining this specialised and valuable digital workforce requires continuous investment in research and development to bridge the gaps between Defence projects. Any interruptions to Defence investment inevitably leads to a loss of workforce from this sector to the commercial digital industry. These losses take years to rebuild and diminish sovereign industrial capability.

Innovation

As a digital industry, this sector is highly innovative and agile, with fast turnaround times and product lifecycles. Software often needs to be developed or updated on a daily or weekly basis, and industry must be able to keep up with this rapid rate of change.

The capabilities captured in this Priority are also supported by artificial intelligence, autonomous systems, cryptography and other advanced digital technologies. An understanding of these technologies will enhance sovereign industrial capability and ensure Defence can make informed decisions when investing in potential innovations.

Defence is working with industry to improve the pull-through of industry research and development breakthroughs into operational capability for the ADF. Innovation funding from the Next Generation Technology Fund and Defence Innovation Hub are promoting research and development, while the recently announced Capability Acceleration Fund will invest over \$130 million from the middle of this decade to support disruptive technologies with industry, and take promising technologies through to acquisition.

Both primes and small and medium businesses understand the importance of investing in research and development and continuing to advance their technology to service both Australian and export markets. Businesses are also diversifying their existing product offerings to increase market share.

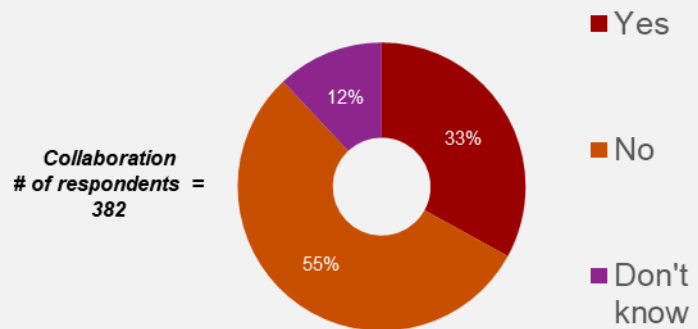
Collaboration

While collaboration does occur, there are opportunities to increase this across the sector.

This industry has complex and niche capabilities that would benefit from collaboration, and deliver greater sovereign technology. Intellectual property ownership, licensing and protection issues can inhibit collaboration and result in unnecessary duplication of effort within industry.

Emerging modular architectures based on open standards can enable a new generation of 'best-of-breed' capabilities built from algorithms, software and hardware sourced from different vendors. This technology trend should represent a significant opportunity for Australian defence industry, especially innovative and agile small businesses, to export their advanced signal processing, and surveillance and intelligence capabilities, to Five Eyes partners.

Primes recognise the valuable contributions small and medium businesses make as innovators, and are working to increase collaboration across the sector to better leverage the dynamic, entrepreneurial mindset in small businesses. Some primes support small and medium businesses by making their accredited research and development facilities – and specialised test and evaluation infrastructure – available to their smaller partners at low or no cost.



Note: Percentage of respondents and whether they have collaborated with another firm or research organisation on an innovation or research and development Defence industry activity

CASE STUDY

Redwing counter-improvised explosive device (IED) force protection systems

The Redwing project, developed in 2016, is an example of Australian industry and defence collaboration, entrepreneurship and innovation to deliver a unique solution that helped address a persistent threat in Afghanistan. The Redwing devices (Greengum and Greygum) were developed by Defence Science and Technology Group, sponsored by Defence's Counter-IED Task Force and manufactured by Australian industry under project coordination by the Australian Military Sales Office. The project included development of two light-weight counter improvised explosive device systems—a handheld version called *Greengum* for use by dismounted troops, and a more powerful system called *Greygum* for fitting to light vehicles.

Under the program, Defence Science and Technology Group and industry partners developed low-cost, robust and lightweight force protection systems for use in austere operating environments by military and police units. The systems function with minimal operator training and limited logistical support. To date, there have been over 100,000 Redwing units delivered to Afghanistan, demonstrating industry's ability to produce and sustain hardware in Australia and support global markets. Industry partners involved in the project included L3 Micro, Ultra Electronics, Associated Electronics Services, AXIOM Precision Manufacturing and Lintek.



Global sector dynamics

Defence recognises Australian industry has capabilities that may provide the ADF and our allies with unique warfighting advantages. It can also benefit from significant export opportunities to our Five Eyes partners who are willing to exchange sensitive military technologies.

Australia continues to use the United States Government's Foreign Military Sales program to procure capabilities, such as aircraft and high-end combat management systems. Australian industry access to intellectual property within these capabilities is required to combine Australian algorithms and software with foreign hardware.

Australian defence industry has a greater capacity for technological innovation than the size of the domestic market can support, creating the need to seek opportunities for exports. The ADF is often too small to justify investment in specific research and development, and some organisations rely on export sales as a larger and more stable revenue stream, in comparison to other markets and customers.

Manufacturing quantities required by the ADF are often too small to justify private sector investment in automation and production. Many Australian businesses therefore rely on offshore manufacturing within an appropriate assurance framework, as the manufacturing of hardware in Australia is unlikely to achieve the economies of scale necessary to compete on price with imported alternative capabilities. In contrast, algorithm and software manufacturing and development is seen as economical to achieve in Australia. However, algorithms and software can never be totally de-coupled from host hardware or firmware, so some sovereign capability to prototype and manufacture limited quantities of hardware is necessary. It is also important that sovereign capability is maintained when tailoring foreign hardware to suit Australian conditions.

Industry consultation

We met with industry, academia and associations representing all parts of the value chain and the full suite of critical industrial capabilities



141

**ORGANISATIONS ENGAGED
INDIRECTLY VIA OTHER
PRIORITIES***



40

ORGANISATIONS ENGAGED

ORGANISATION FOCUS

5

FRIMES

19

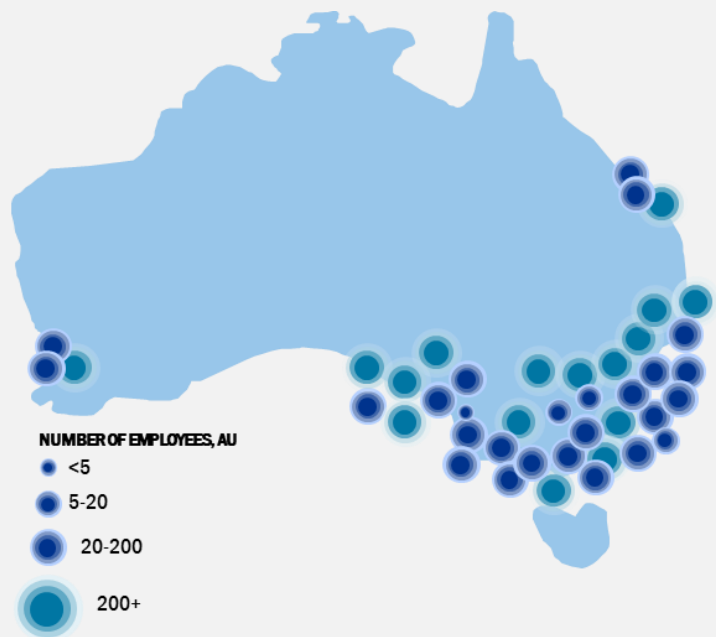
SMEs

30

SOFTWARE

20

HARDWARE



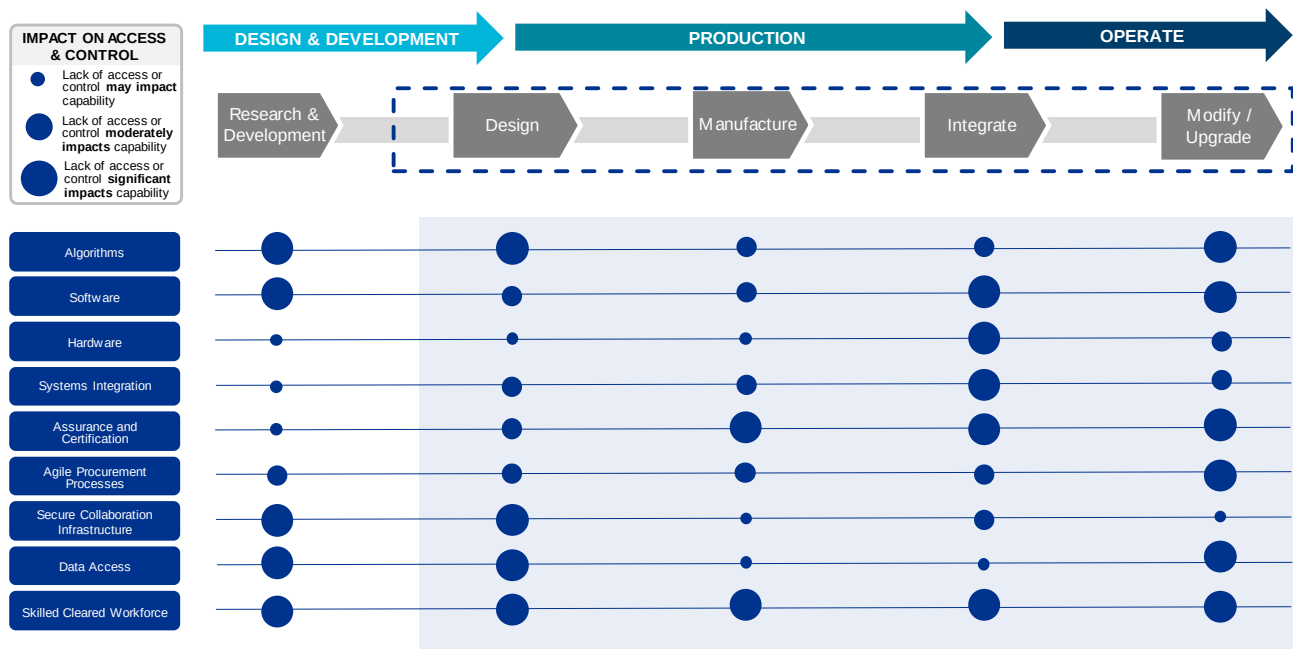
NOTE: Organisations with various locations in Australia have been mapped to their primary location relating to this SICP

* Denotes organisations engaged as part of the Phased Array Radar, Continuous Shipbuilding, Land Combat Vehicles and Aerospace Maintenance SICPs. The insights derived from these consults have had a degree of influence on the insights found in this pack

Value chain

The Defence value chain below presents the activities involved in designing, developing, producing and managing through life support of the capabilities defined within this Priority. In comparison with other Sovereign Industrial Capability Priorities, Advanced signal processing and Surveillance and intelligence have a slightly different value chain, due to the digital nature of these capabilities. It is important to note that 'manufacture' in this value chain includes firmware upgrades, and algorithm and software development, not just hardware manufacturing.

All advanced signal processing and surveillance and intelligence capabilities share a common set of fundamental capability building blocks, which apply to different stages of the value chain. These common components of systems integration, technology (comprising algorithms, software, firmware and hardware), and assurance and certification can each be mapped at different points along the value chain as shown in the figure below.



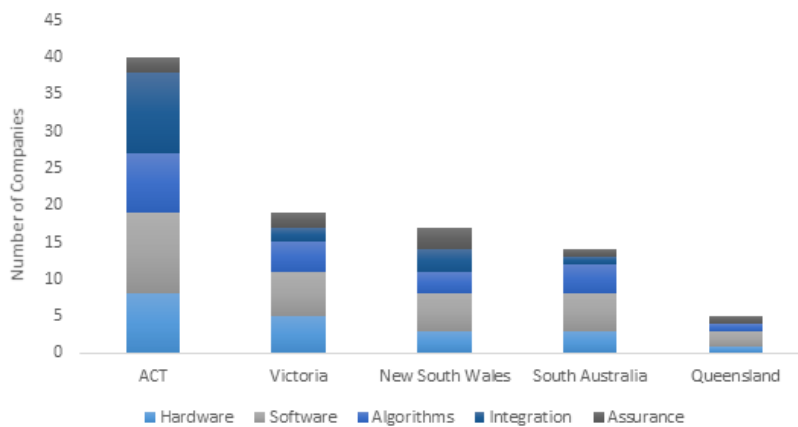
Value chain analysis of this industry sector identified strengths in research and development, software development, and systems and platform integration, which aligns to the needs of this Priority.

National capability overview

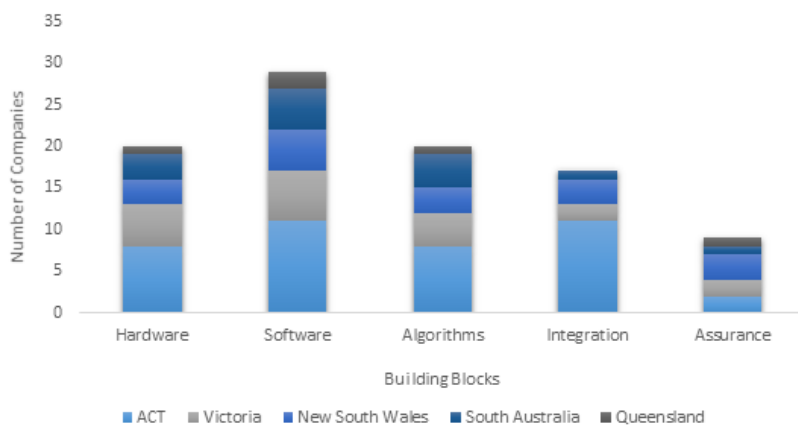
The figures below depict the composition of Australia's advanced signal processing – and surveillance and intelligence industrial capability – based on data gathered during industry consultations and the Centre for Defence Industry Capability survey. Given the sensitive and niche nature of this work, the companies involved work almost exclusively in defence industry.

Numerous insights have been derived through industry engagement in the development of this Plan. Very rarely do companies only contribute to one building block and for the most part, the larger the company, the greater its capabilities against each of the building blocks. Australia's advanced signal processing capability is predominantly based in the country's south and east, with the Australian Capital Territory featuring particularly strongly. This may be a conscious effort on the part of companies to have their head office functions located in close proximity to government agencies, but also may factor in the high number of ex-Defence personnel who are typically employed in defence industry and live in Canberra.

Software is the most represented building block across all states, while hardware and algorithms were the second most featured building blocks. Assurance work featured the least, which may be a symptom of market forces privileging software development as a greater source of capital than assurance and certification of the software. The relationships between the building blocks, to some extent, reveal the composition of companies in this sector. For example, many companies which contributed to the software building block were more likely to also work in integration and algorithms, while none or very few of the companies consulted worked only in hardware or assurance.



The breakdown of capability building blocks across states and territories indicates that this capability has its largest industrial base in Australia's eastern states.



Software development is a critical capability building block for this sovereign capability, and the breakdown of industry reflects its importance. While not all organisations conduct hardware manufacturing or integration, all rely on at least some software development to deliver their products and services.

Workforce and technical skills

The Advanced signal processing and Surveillance and intelligence Priorities both depend on a highly educated digital workforce, competing with global commercial industries for talent. Essential talent in software development and engineering, information technology, data science, and specialist electrical and systems engineering, especially PhD qualifications, coupled with Australian citizenship and the appropriate security clearance, is in exceptionally low supply and high demand. The technical skills required by these two capabilities are rarely developed through undergraduate studies alone, often requiring years of postgraduate studies and on-the-job training.

An understanding of the Defence environment and the requirements of the systems and platforms are also paramount to the success of this industry, which is why defence industry frequently hires ex-military personnel or Australian Public Service employees. Defence is cultivating a digital workforce with the skills needed by this sector to ensure we have the right personnel, and required level of expertise, to enable our success. Building a healthy Defence-to-industry pipeline will help enhance digital technologies throughout the industry, creating and fostering opportunities and innovation.

Many businesses in this sector are looking internationally to find the required talent, which brings its own challenges in achieving the required security clearances. Citizens of other Five Eyes nations can obtain suitable levels of Australian security clearances, albeit after often lengthy processes, but recruiting from other countries is typically not feasible for this sector. A notable proportion of graduates from Australian universities with the digital skills needed by this sector are nevertheless international students who are not able to hold an Australian security clearance.



Industrial processes supporting Sovereign Industrial Capability Priority technologies

This Priority is primarily reliant upon software as opposed to hardware. The ability to update and upgrade software, including the development of algorithms within a sensor, and integrating sensors with other key systems is critical. While an understanding of the underlying hardware is required, advanced signal processing is predominantly reliant on the intellectual know-how of engineers and software developers, as well as telecommunications infrastructure and data centres.

Further, it is important to consider how quickly the digital industry moves. As a digital industry, the underpinning technologies are evolving exponentially, meaning any technical solutions that are developed for today's challenges may not solve the problems of tomorrow. Defence must be flexible and agile to respond to emerging or evolving challenges.

Software development and hardware manufacturing

Given the relatively small scale of domestic demand in Australia, sensor technologies are predominantly built overseas, and many military platforms will be delivered with foreign sensor technologies already integrated in them. Sovereign control will be achieved through the ability to adapt these systems – especially software and algorithms – and integrate them into other technologies to suit the ADF's specific needs and our unique operational environment.

CASE STUDY

Solinnov – BlueBottle Software Defined Radio – the smart phone for EW

The BlueBottle, designed and manufactured by Australian company Solinnov, provides a highly configurable hardware low size, weight, power and cost platform that implements sophisticated software defined radio applications for electronic warfare purposes. Each unit provides radio frequency receive/transmit capabilities and contains embedded processors that allow BlueBottle to sense and affect the radio frequency spectrum. The result is a distributed, networked receiver system that provides electronic countermeasures via software-defined radio to deliver a range of responses against multiple signal modes and characteristics.

Built from proprietary Solinnov firmware and software, Bluebottle is designed to be easily updated and upgraded as Defence needs change. This design results in minimal performance overhead while supporting multi-channel synchronisation and multiple data types across a single link.

The BlueBottle is an example of success achieved through collaboration between Government and industry through the Defence Innovation Hub. BlueBottle was nominated for an innovation award at Pacific 2019, and Bluebottle units are now used by Defence and other Australian national security agencies as sensors.

System integration

Tactical sensors and persistent surveillance systems do not exist or operate in isolation. Tactical sensors must be integrated with military platforms, and systems across all platforms must be integrated with ADF C4I systems. System-level performance can be enhanced through signal processing, but ADF Joint Force capability depends on C4I integration.

System integration is critical to this Priority. The ADF has unique requirements and operates many foreign systems and platforms. The requirement to continually evolve these sensors, and the incorporation of new sensors, means that system integration must be underpinned by an ability to work collaboratively to achieve capability effects. Defence needs Australian industry to successfully integrate advanced signal processing, and surveillance and intelligence capabilities, across the Joint Force.

Open systems architecture understanding

Australia and other Five Eyes partner nations are collectively adopting open systems architectures and technical interoperability standards for tactical sensors, persistent surveillance systems and C4I systems. These new approaches reflect best practice and are also motivated by the need to rapidly change systems and networks to adapt to changing threats and operating environments.

It is essential that Australian industry adopt open systems architectures and Five Eyes technical interoperability standards to ensure their innovations remain fit for purpose for the ADF, and exportable to our partner nations. Failure to adopt these architectures and standards will result in Australian technologies—no matter how independently capable—being unsuitable for integration into ADF and Five Eyes C4I systems, and uncompetitive in domestic and export markets.

Assurance and certification

Assurance of technology components and their certification for ADF use is critical to turning technology into capability. Expertise and understanding around sensor design—and the ability to achieve high levels of assurance and meet the required certification standards—are critical to this capability. This is because most system hardware will likely continue to be manufactured overseas. It is acceptable to have mission critical systems that include foreign technology components, so long as Australia has control of its integration, assurance and certification.

This Priority relies on ensuring the appropriate level of control over foreign hardware and platforms. We need to guarantee that foreign-sourced technology can operate in the unique Australian environment and behave within certain performance criteria. While this objective is achievable for foreign manufactured hardware, it is very difficult to reach the same level of assurance with foreign developed software. For this reason it is important to retain the software development capability onshore.

The assurance and certification capability:

The *Test, evaluation, certification and systems assurance* Industry Plan will deepen industry's understanding of the requirements for assurance and certification to support sovereign capabilities. It is recognised as a key building block for both the Advanced signal processing and the Surveillance and intelligence Priorities

Signature management

Signature management is a critical industrial capability in this Priority. Defence has historically developed most of its signature management solutions in-house through Defence Science and Technology Group. Furthermore, most foreign sourced military platforms are delivered to the ADF with extensive built-in physical signature management features not easily accessible to Australian industry.

Electronic and digital signature management technologies are rapidly growing in importance to the ADF and there is significant opportunity for Australian industry to contribute to this emerging capability. Defence recognises the export market for this capability is likely to be highly limited due to the sensitivity of signature management technologies. Given the historical role of Australian defence industry in signature management and the limited commercial viability of ramping up this critical industrial capability, Australian companies will need to work together to build this sovereign industrial capability.



Assets and infrastructure

This Priority highlights the importance of access to, and control over, certain components of infrastructure to achieve advanced signal processing capabilities. This requirement can include assured access to anechoic chambers, controlled electronic warfare ranges, controlled bodies of water for sonar testing, and access to sovereign data centres and telecommunications networks. Anechoic chambers are used for near and far field testing of antennas and radio frequency components. Controlled radio frequency ranges exist within Defence-controlled land, providing the necessary infrastructure to emulate a threat-representative signals environment.

In cases where this infrastructure already exists, Australia has been able to advance its signal processing capabilities. Access to large bodies of controlled water enables Australian companies to conduct ground-breaking research into towed arrays. Sovereign data centres and telecommunications networks involve Australian-controlled ICT infrastructure suitable for transporting, processing, and storing sensitive and classified data. These examples highlight how the development of these highly technical capabilities is only as effective as the infrastructure supporting it.



Australian defence industry as a global leader

Australia is well placed with the requisite talent and infrastructure to conduct world-leading research and development in advanced signal processing, and Australian defence industry has the technical expertise to lead global best practice. Complex systems integration of diverse foreign technologies is an area of Australian defence industry expertise that is highly sought after by many nations with militaries of comparable composition and size to the ADF. The extent to which the United States and United Kingdom look to Australian defence industry to contribute niche advanced signal processing capabilities to their much larger militaries attests to our position as a global leader in this sector.

CASE STUDY

Thales Australia – Underwater acoustic testing

Thales Australia has entered into a Memorandum of Understanding (MOU) with the Australian Maritime College (AMC), University of Tasmania in Launceston and Australian SME partner AMOG to conduct the test, trial and acceptance of Towed Array technologies in the highland lakes of Western Tasmania. These technologies are a critical element of Australia's ongoing submarine capability, as well as frigate and undersea surveillance programs, and this partnership will deliver a world-class facility that complements the Tasmania's new Defence and Maritime Innovation and Design Precinct.

A key outcome for the facility is ensuring a steady state of utilisation and support to a range of academic and SME service suppliers in the region. As such, the facility has incorporated current and emerging Defence related requirements including proof of concept, test and validation of Integrated Undersea Surveillance Systems technologies.

Requirements from adjacent industries and research organisations, including deep-water towed system trials for the Australian Antarctic Division vessel RSV Nuyina have also been accommodated to ensure this unique capability within Australia remains a commercially successful facility for decades to come.

Australia's strategic relationships with other nations, especially Five Eyes partner nations, governs the extent to which Australian defence industry can access global markets. The Five Eyes military export marketplace is relatively closed and protected, offering significant advantages to Australian businesses seeking to broaden their customer base beyond the ADF. If Australia continues to invest and develop new and innovative technology, there will be opportunities to leverage the relationship with partner nations and increase our advanced signal processing capabilities.

Risks to domestic industry

Industry consultations revealed several risks to this industry sector in Australia. The need to obtain and retain engineering knowledge, competition with global markets, and challenges with economies of scale will need to be addressed to achieve long-term success in this industry.

Access to secure facilities and information and communications technology

A critical component in the ongoing development of advanced signal processing technology is access to specialised infrastructure to test sensor functionality, and Defence Secret Network test enclaves to test sensor integration to C4I systems.

Research and development of sensitive technologies often must be conducted in specialist facilities using accredited secure information and communications technology. Accreditation of facilities can take over two years and cost hundreds of thousands of dollars which may deter new businesses from entering the defence industry. This is a significant barrier for the growth of the advanced signal processing capability. Industry needs to consider working together to develop joint-user facilities, as well as secure cyber environments, to develop, test and modify their sensitive software and technologies.

Access to the right skills

The workforce in this sector requires tertiary education in relevant technical disciplines at a minimum, and a large proportion of the workforce requires PhD qualifications. Australian defence industry must compete with global digital technology giants such as Google, Microsoft and Amazon for talent graduating from Australian universities.

Defence is reviewing security clearance processes and perceptions to ensure they do not deter graduates from joining defence industry. Many Australian graduates move overseas to start their careers in the digital industry. Further, non-Australian graduates from Australian universities may be unsuitable for recruitment due to security clearance requirements. It was noted during industry consultations that organisations often need to invest in significant on-the-job training to develop the required skills and capabilities for their operations.

One of the most significant risks to this industry is the need to obtain and retain engineering knowledge, specifically in software development and data fusion, to build a home-grown community of expertise. Defence industry is competing with large technology companies for the best talent, who are global in their remit, without the added complexities of citizenship or security clearance requirements. The inability to access specialised engineering knowledge could limit Australia's ability to expand a sovereign industrial capability in the advanced signal processing sector. Potential employees including software engineers, specialist discipline engineers, software developers, data scientists and data engineers are highly sought after, but face lengthy periods of processing to obtain security clearances. Further, after obtaining security clearance, there is no guarantee of long-term employment.

The need for greater collaboration

A common theme across industry consultations was a sense of limited collaboration with other participants in the supply chain. There is a perceived absence of a secure and trusted platform to truly collaborate, meaning organisations are investing in, and developing, siloed concepts or products. Organisations working in isolation often pull in different directions and inhibit innovative ideas transitioning into service solutions. Collaboration is particularly critical for systems integration and networking dissimilar sensor types and models. Defence recognises the value of collaboration in this sector and the Defence Innovation Hub will continue collaborating in the sector, where possible.

Global trade barriers

The sensitivity of advanced signal processing and surveillance and intelligence technologies typically limits the export market to Five Eyes partner nations. The United States is the biggest market, but also the most challenging to do business with due to the complexities of its International Traffic in Arms Regulations and associated Technical Assistance Agreement requirements. Australian industry must compete with global businesses that enjoy greater economies of scale and access to cheaper labour and materials. Specific to signature management technologies, many Australian industry products will be tailored to military platforms and may also be so sensitive they cannot be exported.

The critical importance of Five Eyes interoperability is driving adoption of Five Eyes technical standards and open systems architecture approaches. These standards and architectures facilitate greater levels of machine-to-machine data exchange between diverse sensors and C4I systems dispersed across the networked Joint Force. These improved data flows enable networked sensor fusion and highly distributed real-time data processing, exploitation, dissemination and presentation, both contributing significantly to ADF warfighting advantage.

Defence requires Australian industry to adopt and implement these Five Eyes technical standards to the greatest extent possible to support interoperability-by-design in the ADF. However, the Australian Government cannot release some of these technical standards to Australian industry entities with non-Five Eyes foreign ownership or controlling interests. Without access to the necessary technical information, industry will experience a competitive disadvantage in the Australian and wider Five Eyes defence industry marketplace, no matter how independently capable their technologies or solutions may be.

Security

Threat actors seek access to privileged information in relation to Australia's military capabilities. Advanced signal processing capabilities present high-value targets. Members of defence industry need to maintain awareness and uphold Defence's security principles to protect the military capabilities they contribute to, including:

- Information Security – industry partners must understand the value of the information they hold, where it is stored, and how it may be accessed; ensure cyber and cloud-based security has been certified in accordance with the Defence Security Policy Framework; and not post sensitive information on public or social media forums.
- Personnel Security – industry partners must regularly brief their workforce on threat and security issues; maintain adequate personnel security, including the use of passes and visitor escorts; and understand the correct reporting procedures for any security incident or suspicious contact.
- Physical Security – industry partners must ensure facility security zones are appropriately assessed and certified; maintain effective access control systems; and only admit access to people who have a genuine need to know.

Defence requires all industry entities to hold an appropriate level of Defence Industry Security Program (DISP) membership when working on sensitive or classified information or assets. Defence provides DISP members with security support, including personnel security vetting information, certification and accreditation of facilities, and information and cyber technology systems. This enables industry to ensure their security practices are 'Defence-ready'.

BUILDING INDUSTRIAL CAPABILITY

Two Sovereign Industrial Capability Priorities, one digital industry sector

Linking different, but closely related areas of Defence capability, the Advanced signal processing and Surveillance and intelligence Priorities share the same industrial base with a common set of industrial capability enablers. Organisations in this industry rely on a common workforce and common infrastructure to deliver the critical industrial capabilities. The enablers listed below support this industry and enhance Australia's sovereign industrial base.

Industry capability enablers

Through broad consultation with Defence and industry stakeholders, analysis of the value chain—and consideration of the ADF's strategic ambitions and outlook—four driving enablers for the Advanced signal processing Priority have been identified.

The industry capability enablers and the associated government actions detailed in this section are common across both the Advanced signal processing and Surveillance and intelligence Priorities.



AGILITY WITHIN THE SECTOR

Defence industry must be agile and flexible to ensure that ADF technologies, sensors and capabilities can keep pace with the rapid refresh rate in these industries, and the changing security landscape. To maintain the ADF's warfighting advantage, industry must be flexible to cater to software and software-defined hardware that may need to be updated daily or weekly. This requires agility from both Defence and industry to rapidly pivot and deliver software engineering solutions to meet the ADF's needs.

Agility within the defence industry sector ensures the ADF has the advanced signal processing and surveillance and intelligence capabilities to meet current and future needs. A key component of industry's agility is an awareness of upcoming Defence projects and capability needs, and a suitably skilled and cleared workforce.



Government action

Industry engagement days

Defence will host industry engagement days to inform stakeholders on current and emerging Defence capability requirements—as well as information on security requirements and tendering processes—to help new defence industry businesses. Industry engagement days will occur through the next two years and will be advertised through Austender and the Defence website.



SECURE COLLABORATION INFRASTRUCTURE

Valuable and sensitive advanced signal processing, and surveillance and intelligence capabilities must be protected throughout the entire value chain from compromise by a potential adversary. Accredited, secure physical infrastructure (secure facilities), and information infrastructure (secure computer networks) are essential for Australian defence industry to meaningfully contribute to this Priority.

Traditionally there is significant expense and lead time to accredit new facilities and networks. This considerable barrier to entry has resulted in only very established industry members having accredited infrastructure and limits the growth of new businesses in the sector. Collaboration and information sharing between industry has also been impeded as businesses are not using common operating systems, software and networks. This lack of collaboration can create a barrier for early stage research and development.

Modern Cybersecurity Frameworks

In January 2020, the US Department of Defense released the Cybersecurity Maturity Model Certification (CMMC) version 1.0. The framework was developed in a collaborative process with university-affiliated research centres, federally funded research and development centres, and industry.

The CMMC brings together a number of previously discrete compliance processes into one unified framework. The biggest change for industry under the CMMC will be the necessity to subject themselves to external security audits, which up until now, could be done internally. Meeting these standards will be an essential requirement to supply to the US Department of Defense. This will be a critical issue for Australian companies to consider, given that export opportunities in this portion of defence industry are often constrained to the Five Eyes community.



Government action

Cyber readiness

The Australian Department of Defence will support businesses who contribute to one or more of the Sovereign Industrial Capability Priorities to align their cyber-security processes to meet new international frameworks through the Sovereign Industrial Capability Grants program. These international cyber-security processes will ensure Australian industry can continue to export to the US and actively participate in global markets.



DATA ACCESS

Data access is an important enabler to developing machine learning and other artificial intelligence techniques for signal and data processing. Without access to Defence data, businesses in the sector must develop solutions to presumed problems using surrogate data. The result is suboptimal products that require significant adaptation if adopted by Defence.

Defence industry access to real Defence data, such as recorded sensor data, threat intelligence, and technical information, also helps support and enhance research and development, allowing industry to create solutions for the obstacles and threats facing the ADF.

Five Eyes interoperability is a critical requirement for military systems and platforms. Data formats and exchange mechanisms between networked sensors are defined by various Five Eyes technical standards controlled by partner nation governments. Defence expects Australian industry to design digital signal processing, sensor fusion, and other real-time data processing algorithms and software that comply with relevant standards and ensure interoperability by design.



SKILLED CLEARED WORKFORCE

A highly educated and skilled workforce with the necessary levels of security clearance and a good understanding of Defence missions and needs is an important enabler of this Priority.

The level of training and experience required to develop leading-edge sensor and signal processing capabilities requires significant investment in postgraduate studies and on-the-job training. Likewise, the ability to re-train or transfer skills across multiple technologies or platforms is challenging and not as simple as in other industries.

There are mechanisms in place to help industry obtain security clearances for their workforce, but obstacles can arise in the time taken to complete the clearance process. Defence is exploring opportunities to offer industry more unclassified work packages that build business confidence to invest in recruiting and clearing the workforce.

Platforms and technologies that deliver advanced signal processing capabilities will continue to be replaced and upgraded. Workforce knowledge and experience will be critical to ensuring a long-term capability in Australia. Essential talent in software development and engineering, information technology, data science, and specialist engineering is a key enabler.



Government action

Skilled workforce development

To support workforce development in advanced signal processing capabilities, Defence will provide grants to small and medium businesses through the Skilling Australia's Defence Industry Grants Program. This supports upskilling and training opportunities and builds skills and capability to meet current and future Defence needs.

More, Together. Defence Science and Technology Strategy 2030

Defence Science and Technology Group released the *More, Together. Defence Science and Technology Strategy 2030*, to deliver greater impact through large scale activities, supported by a national science and technology enterprise and international partnerships.

The strategy includes three pillars. The *Brilliant People, Collaborative Culture* pillar focuses on developing a highly skilled, innovative, collaborative and inclusive workforce to meet the science and technology challenges of delivering a capability edge for Defence. By implementing Defence's Science, Technology, Engineering and Mathematics Strategic Vision, this pillar will be supported by a set of key workforce objectives that will shape, partner, inspire, promote and retain skills.

Defence Industry Skilling and STEM Strategy

Defence has recognised the need to take a stronger role in collaborating across government, industry and academia to secure a strong and diverse technology enabled talent pool. The *Defence Industry Skilling and STEM Strategy*, released February 2019, provides specific guidance and funding support for Defence Industry skills needs.

Building a signature management industry in Australia

Reducing and manipulating the signatures of military platforms is critical to assuring their lethality and survivability in a contested battlespace, especially as our potential adversaries advance their sensor technologies. Hiding military platforms from detection, tracking and targeting requires an integrated approach to signature management.

The Collins class submarine maintenance and technology upgrade, Aerospace platform deeper maintenance and Land combat vehicle and technology upgrade Industry Plans all highlight the importance of military platform signature management in maintaining ADF warfighting advantages. Different aspects of physical signature management are more or less important to different platforms based on their operating environments. For example, reducing acoustic and magnetic signatures is critical to submarines but not to aircraft, while reducing radar cross section is critical to both aircraft and submarines.

In contrast, electronic and digital signature management are critically important to all military platforms, and these signatures can be protected using software-defined systems added in later stages of the value chain. For example, a radio frequency emissions monitoring and control system could be added to a platform to reduce or manipulate its electronic signature. This type of signature management capability is rapidly growing in importance as control of the electromagnetic spectrum becomes a critical warfighting advantage.

The highly sensitive and valuable nature of military platform signatures makes signature management technologies highly classified and limits export opportunities. Appreciating that the domestic market for these technologies is currently small and that Australian industry may find it difficult to achieve the economies of scale necessary to make their solutions competitive on price, Australian industry needs greater access to military platform data to enable the research and development of innovative new electronic and digital signature management technologies.

ANNEX A. GOVERNMENT ACTIONS

This Plan includes the following actions to be taken by Defence to support this Priority. Although responsibility has been attributed to a particular branch, group or agency, it is expected that a broader group of Defence and Government stakeholders will participate in, or contribute to, the action.

Title	Government Action	Responsible	Timeframe
Industry Engagement Days	Defence will host industry engagement days to provide industry stakeholders with information on current and emerging Defence capability requirements, as well as information on security requirements and tendering processes to help businesses new to defence industry. Industry engagement days will occur throughout the next two years and will be advertised through Defence and Austender.	Joint Capabilities Group / Capability Acquisition and Sustainment Group	Ongoing
Cyber Readiness	The Australian Department of Defence will support businesses who contribute to one or more of the Sovereign Industrial Capability Priorities to align their cyber-security processes to meet new international frameworks through the Sovereign Industrial Capability Priority Grants program. These international cyber-security processes will ensure Australian industry can continue to export to the US and actively participate in global markets.	Strategy, Policy and Industry Group	Until 30 June 2022
Workforce Development	To support workforce development in advanced signal processing capabilities, Defence will provide grants to small and medium businesses through the Skilling Australia's Defence Industry Grants Program. This supports upskilling and training opportunities and builds skills and capability to meet current and future Defence needs.	Industry Policy Division	Until 30 June 2022

ANNEX B. SUPPORT THROUGH INDUSTRY PROGRAMS

This section discusses the support available to current and aspiring Defence industry in support of this Sovereign Industrial Capability Priority and other Defence capabilities.

Defence innovation system

The Centre for Defence Industry Capability, the Defence Innovation Hub and the Next Generation Technologies Fund comprise the integrated Defence innovation system, helping encourage innovation and growth in the Australian industry. This system will support companies that contribute to this Priority to further innovate, and position themselves to better support the ADF. The *2020 Force Structure Plan* aims to better bridge the divide between technology development and acquisition by strengthening the link between Defence's capability plans with industry policy initiatives, Defence's reform program, the *More, Together: Defence Science and Technology Strategy 2030* for innovation, and clear resourcing plans. These programs have been bolstered by various measures in the Government's economic recovery package; aimed at supporting economic recovery from COVID-19 through targeted investment in key manufacturing, construction and high-tech sectors of defence industry, and increased funding for Defence innovation, industry grants, and skilling.

Centre for Defence Industry Capability

The Centre for Defence Industry Capability remains the entry point for Australian businesses either working in or looking to enter the defence sector. They provide advice to industry on what initiative will best assist them, depending on their stage of product development. The Centre has specialist business facilitators situated in capital cities around Australia who can be contacted to discuss opportunities related to this Priority. The Centre also provides guidance on business improvement, skills development, Defence market preparedness, and export and supply chain support.

The Centre administers multiple grant programs, including:

- **Capability Improvement Grants** of between \$4,000 to \$240,000 for small-to-medium enterprises to fund part of the cost to engage a consultant or expert to assist with skills and training, build the capability of the existing workforce, and meet specific business needs. Under the *Defence Industry Skilling and Science, Technology, Engineering and Mathematics Strategy*, the Centre will be offering skilling support grants to defence industry small-to-medium enterprises to reduce barriers of skills and retraining their workforce.
- **Defence Global Competitiveness Grants** of \$24,000 to \$240,000 for small-to-medium enterprises to fund up to half the cost of projects that are building their defence export capability. The grants aim to promote a stronger, more sustainable and globally competitive Australian defence industry.
- **Sovereign Industrial Capability Priority Grants** program was established in November 2018. The grants program allows Defence to improve the resilience of a Priority by providing funding to industry to ensure that Australian small-to-medium enterprises have the appropriate capacity and resilience to support Defence's critical capabilities. Grants of up to \$1.4 million are available to fund capital equipment purchases (including specialist software and security infrastructure), non-recurring engineering costs, design activities directly related to the project; and workforce training and accreditation directly related to the project. The grants are capped at \$4.2 million over three years. These grants directly subsidise the growth of industrial capabilities underpinning the Priorities and are for more mature companies that are able to fund at least 30 per cent of the funding.
- **Skilling Australia's Defence Industry** grants provide businesses servicing the defence sector with funding of up to \$500,000 to undertake upskilling and training opportunities to build skills capacity and capability to meet current or future Defence needs. These grants will reduce the barriers faced by defence industry in upskilling or retaining their people, by offering financial support for training in trade, technical and professional skillsets.

More information is available at: <https://www.business.gov.au/CDIC/Grants-for-defence-industry> and <https://www1.defence.gov.au/business-industry/skilling-defence-industry/stem-support>

Defence Innovation Hub

The Defence Innovation Hub brings together defence industry, academia and research institutions to collaborate on innovative technologies that can be developed into capability for Defence. Funded at over \$800 million over the next decade, the Defence Innovation Hub accepts proposals that are ready to enter the engineering and development stages of the innovation process, from concept exploration and technology demonstration to prototyping and integrated capability demonstration and evaluation.

Each year, the Hub reviews and publishes its innovation priorities to help innovators plan their research and development activities. The Defence Innovation Hub's innovation priorities align with Defence's capability programs, and the most relevant for this Plan are Intelligence, Surveillance, Reconnaissance, Electronic Warfare, Space and Cyber.

More information is available at: <https://www.business.gov.au/centre-for-defence-industry-capability/defence-innovation/defence-innovation-hub/defence-innovation-hub-priorities>

Next Generation Technology Fund

Science and technology is a significant priority for Defence. Defence has to be prepared for the next revolution in the way war is fought. To do this, the Government has invested more than \$164 million in 204 research activities and will make further investments worth approximately \$1.2 billion over the next decade, through the Next Generation Technology Fund. This forward-looking program focusses on research and development in emerging and future technologies for the 'future Defence Force after next'.

The Next Generation Technology Fund supports a number of collaboration initiatives such as the Emerging Disruptive Technology Assessment Symposium and the Grand Challenges. These aim at getting the best thinkers in Australia on a particular topic together and facilitating collaboration between Defence, industry and academia. There are also a number of funding initiatives managed through the Next Generation Technology Fund that companies who contribute to this Priority may wish to leverage. These include:

- **The Small Business Innovation Research for Defence program:** provides opportunity to Australia's small-to-medium enterprises to undertake research projects that will benefit Defence in the future. Successful project outcomes might be commercialised directly by the participant, be the subject of a separate development support application with the Defence Innovation Hub, or be adapted to support other Next Generation Technology Fund ventures such as a Grand Challenge.
- **Emerging Disruptive Technology Assessment Symposium** is a Defence Science and Technology Group driven series of invitation only events, in partnership with universities and industry. Aligning with the priority areas of the Next Generation Technology Fund, the Symposium facilitates the strategic planning of technology that is understood to evolve Defence and National Security domains over the next 20+ years.
- **Grand Challenges Program:** brings together small, agile companies, large organisations, and academic researchers with Defence Science and Technology Group scientists to collaborate and find solutions for highly complex strategic defence and national security challenges. The first Grand Challenges was centred on Counter Imposed Threats which awarded contracts to 21 organisations to develop prototypes of a threat detection and defeat system through collaboration.
- **The Small Business Exploratory Program:** accelerates promising science and technology of interest to Defence, from early-stage concept to a point where a proposal could be submitted to the Defence Innovation Hub.
- **Defence Cooperative Research Centres Program:** focussed on selective next generation research and development projects and high-priority Defence capability needs. It is delivered through a collaborative network of industry organisations (particularly small-to-medium enterprises), researchers and Defence.
- **Strategic Research Program** aligns Defence's strategic priorities with emerging technology and new concepts, such as cyber. This is led through Defence Science and Technology Group, providing opportunities for industry and academia in collaboration.
- **Technology Futures and Foresight Program** brings together industry leaders and academia to consider emerging challenges and opportunities that will materially influence Defence's future vision. Based on this assessment, the Program establishes initiatives, such as the Emerging and Disruptive Technology Assessment Symposium, to create dialogues, partnerships and a deeper understanding of the current and future operating environment.

More information is available at: <https://www.dst.defence.gov.au/NextGenTechFund>

Capability Acceleration Fund

To ensure Defence's innovation system has the capacity to meet the demands of future technological development, a new Capability Acceleration Fund will be introduced from the middle of this decade. Through this fund the Government will invest over \$130 million to support the intensive development of key disruptive technologies with industry beyond the early-stage research and demonstration stages, taking promising technologies all the way through to acquisition. This is intended to bring

together industry participants, Defence personnel and technical subject-matter experts to provide the support needed to build prototypes to demonstrate capability and set requirements for future projects.

More information is available at: https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf

Other Defence support opportunities

Australian Defence Export Office

The research, consultation and analysis undertaken to develop this Plan provided evidence of the number of Australian companies already pursuing export opportunities or supplying to overseas customers. The Defence Export Strategy intends to support these companies in their endeavours, and to encourage more small to medium enterprises to pursue export opportunities.

The strategy, released in 2018, outlines the Government's plan to support Australian defence industry to achieve greater export success to build a stronger, more sustainable and globally competitive defence industry to support Australia's Defence capability needs. Increasing access to international markets through exports will assist in reducing the risk to industry of having a single customer in the ADF. It will also support industry's ability to sustain and grow business through the peaks and troughs of domestic demand.

The Australian Defence Export Office provides a focal point for delivering the key initiatives of the strategy. The Office provides a coordinated approach to export support, working closely with Austrade, the Centre for Defence Industry Capability, Department of Foreign Affairs and Trade, the Export Finance Australia, state and territory governments, and Australian defence industry, to realise export success.

The ADEO tailors support to industry on a case-by-case basis, including through the Australian Military Sales, Team Defence Australia, and policy and engagement functions. The Australian Defence Export Office leads several initiatives to support Australian defence industry:

- international advocacy for Australian defence industry exports;
- support from the Australian Defence Export Advocate, including international advocacy;
- assistance from dedicated business development managers in key markets;
- attendance at Team Defence Australia trade shows;
- targeted international trade missions;
- government-to-government sales and transfer of equipment;
- inclusion in the Australian Military Sales Catalogue;
- Defence Global Competitiveness Grants (administered by the Business Grants Hub);
- Landing Pads (administered by Austrade);
- Defence Export Facility (administered by Export Finance Australia); and
- market intelligence.

All companies seeking Australian Defence Export Office support should be aware of their Defence export control obligations.

More information is available at: <https://www1.defence.gov.au/business-industry/export>

National Defence Industry Skills Office

The National Defence Industry Skills Office is implementing the initiatives announced in the 2019 Defence Industry Science, Technology, Engineering and Mathematics Strategy. The Strategy details how the government will help Australian defence industry meet their workforce skills requirements over the coming decade. The National Defence Industry Skills Office will align efforts to ensure access to essential skills relating to Sovereign Industrial Capability Priorities. Initiatives companies can leverage include:

- the Skilling Australia's Defence Industry Grants Program, administered through the Centre for Defence Industry Capability, which focuses on improving accessibility for small to medium businesses and reducing the barriers faced by defence industry in up skilling or retraining their people;
- the Schools Pathways Program, which encourages student engagement in science, technology, engineering and mathematics and introduces them to the many career pathways in defence industry; and

- the Defence Industry Internship Program, which includes 70 students per year. This will provide engineering students with direct connections to defence industry by facilitating 12 week internships with industry small to medium businesses.

The Defence Industry Internship Program

The Defence Industry Internship Program links third and fourth-year engineering students with Defence sector small to medium businesses by sponsoring the industry placement component of their studies. The program specifically targets the engineering streams that defence industry consider to be in short or critical supply and aims to give student engineers a better understanding of the critical work performed by our defence small to medium businesses.

More information is available at: www.business.gov.au/centre-for-defence-industry-capability/news-events-and-resources/skilling-and-stem-strategy and www.diip.com.au

Defence Civilian Undergraduate Sponsorship

The Defence Civilian Undergraduate Sponsorship aims to attract students to undertake a degree through the University of New South Wales Canberra campus at the Australian Defence Force Academy. This is a civilian-based sponsorship, with no military service obligations or requirements, open to those who may be interested in a career in the Department of Defence.

The Department of Defence runs this program annually, and the undergraduate degree disciplines offered are subject to change. In 2021, applications are expected to be sought for the following disciplines:

- Bachelor of Engineering (Mechanical, Electrical, Civil and Aeronautical) (4 years)
- Bachelor of Computing and Cyber Security (3 years)

The Defence Civilian Undergraduate Sponsorship offers coverage of the full tuition costs for eligible applicants, plus an annual allowance to cover the cost of textbooks and equipment.

During the sponsorship, students may have the opportunity to participate in paid work placements within Defence which will provide exciting opportunities and give an insight into how one of Australia's largest organisations conducts business.

More information is available at: <https://www1.defence.gov.au/jobs-careers/civilian-undergraduate-sponsorship>

Global Supply Chain Program

The Global Supply Chain Program seeks opportunities for Australian industry, particularly small to medium enterprises, within the supply chain of multinational defence primes. Through the Centre for Defence Industry Capability, this Program facilitates Australian industry capability with the commercial needs of the eight prime contractors involved in the Global Supply Chain Program. Those are BAE Systems, Boeing, Leidos, Lockheed Martin, Northrop Grumman, Raytheon, Rheinmetall and Thales.

The eight primes are funded to establish Global Supply Chain teams to identify business needs and provide access to these to Australian companies, qualify eligible Australian supply chain contenders, provide ongoing support and feedback and work alongside other primes to boost exports and uplift the small to medium enterprise.

Defence TAFE Employment Scheme

The Defence TAFE Employment Scheme aims to assist students looking to pursue a career in Defence by supporting their vocational education with practical, paid work experience. Defence TAFE Employment Scheme participants work part time within the Australian Public Service while studying, and are remunerated with a full-time salary.

In 2021, applications are expected to be sought for the following disciplines (subject to change):

- Victoria: Logistics / Business Administration / Leadership and Management / Engineering (Mechatronics, Mechanical, Software Communications, Telecommunications, Electrical, Electronics)
- Australian Capital Territory: Business / Computing and Cyber Security / Database Design and Development / Engineering (Electrical, Industrial Electronics, Renewable Energy, Systems, Technical) / Government / ICT and Networking / Logistics / Purchasing, Procurement and Contracting / Software Development / Website Development
- New South Wales: Logistics / Database Design and Development / Engineering (Electronics, Electronics and Communication, Instrumentation and Control) / ICT and Networking / Software Development / Website Development
- Western Australia: Computing and Cyber Security / Engineering (Electrical, Electrotechnology)
- South Australia: Engineering (Electronics, Communications) / Logistics

More information is available at: <https://www1.defence.gov.au/jobs-careers/TAFE-employment-scheme>

External support and collaboration opportunities

Industry are able to access further support and collaboration opportunities with respect to the Surveillance and intelligence Priority through the organisations below. The list provided below is intended to focus on those opportunities specific to the Priority and not intended as exhaustive. It is acknowledged that other schemes and programs are available at academic institutions and across industry.

The Modern Manufacturing Strategy

Make it Happen, the Australian Government's Modern Manufacturing Strategy notes the importance of the manufacturing for Australia, and outlines a range of activities the Government is delivering to drive productivity and create jobs for Australians, both now and for generations to come. Defence is listed as one of the six National Manufacturing Priorities, highlighting the importance of defence industry to the broader manufacturing sector.

More information on the Modern Manufacturing Strategy, including individual initiatives and support for business, can be found at <https://www.industry.gov.au/data-and-publications/make-it-happen-the-australian-governments-modern-manufacturing-strategy>

Commonwealth Scientific and Industrial Research Organisation (CSIRO)

The CSIRO is a government organisation with a focus on using innovative science and technology to solve complex challenges. The CSIRO works across all sectors with companies of all sizes, both in Australia and overseas to produce tangible commercial products and solutions, generating circa \$3.2 billion per annum in benefits from these collaborations.

CSIRO offers a range of programs and funding streams such as:

- **Small to medium enterprise Connect:** a dollar-for-dollar matched scheme, available to Australian small to medium enterprises turning over \$100 million or less per year wanting to undertake research projects. This program aims at helping small to medium businesses to undertake research and development. Small to medium enterprise Connect works with a business to: identify the problem; locate the right research capability; develop relationships with research organisations assist development and design of the project; apply for grants or funding; facilitate project agreements and assist with contracting.
- **Commonwealth Scientific and Industrial Research Organisation Innovation Fund:** facilitates attracting private funding, and invests in high technology industries in support of technological advancements.
- **Innovation Connections:** enables small to medium businesses to receive funding and support to engage researchers. Under this program, industry can receive support to have a researcher embedded into their business, have a researcher from the business placed into public research organisations such as Commonwealth Scientific and Industrial Research Organisation, or have a graduate undertake a research project within the business.
- **Uniseed:** a commercialisation venture fund operated through Commonwealth Scientific and Industrial Research Organisation, supporting universities across Australia in incubating technological ideas into products and services.

More information is available at: <https://www.csiro.au/>

Innovation Connections

The CSIRO and the Australian Government have established a new program which enables small to medium businesses to receive funding and support to engage researchers. Under this program, industry can receive support to have a researcher embedded into their business, have a researcher from the business placed into public research organisations such as the CSIRO, or have a graduate undertake a research project within the business.

State-based Defence Research Networks

Over the last decade, a series of State government sponsored defence research networks has evolved with a remit to help support their local universities and industries connect into a globally engaged, competitive and innovative defence and national security sector. These networks are co-supported by DST to work together on shared programs in support of the national endeavour.

The networks themselves do not undertake any research. Instead, they facilitate university-government-industry research and skills exchange by actively cultivating relationships and linkages, including:

- enhancing Defence relevant research and development engagement between universities, industry and Defence;
- identifying Defence relevant research and technology development opportunities on behalf of our stakeholders;

- providing advice on the Defence research and development environment (priorities, capabilities, needs and gaps);
- connecting small businesses to research and expertise in order to strengthen participation in Defence business; and,
- promoting and showcasing research and development and innovation in the private and public sectors.

The state-based Defence Science University Networks currently include the Defence Science Institute (DSI) in Victoria; the Defence Innovation Partnership (DIP) in South Australia; the Defence Innovation Network (DIN) in New South Wales and Defence Science Centre (DSC) in Western Australia (see Table 1). The Queensland Defence Science Alliance (DSA) is in the process of setting up its state-based network and is expected to be up and running in Q3 2020. The state-based Defence Science university networks are funded by three distinct funding streams: state governments; Defence; and university stakeholders.

The State-based Defence Research Networks

	DSI	DIP	DIN	DSC
State	VIC	SA	NSW	WA
Establishment	2011	2017	2017	2019
Lead entity	University of Melbourne (UoM)	Defence SA	University of Technology Sydney	Department of Jobs, Tourism, Science and Innovation
Number of University partners	8	3	7	4
affiliated state government department	Department of Jobs, Precincts & Regions	Defence SA	Office of the Chief Scientist and Engineer and Defence NSW	Department of Jobs, Tourism, Science and Innovation

Defence Science Partnerships with Universities

Defence Science and Technology has reinforced the capacity to partner with Australian universities through a new Defence Science Partnerships Framework, DSP2.0. This framework provides a foundation to build collaborations between Defence and universities. It provides flexibility in partnering arrangements, provisions for multi-party collaborations, enhanced security and bespoke arrangements for large strategic projects. Every public Australian university has signed this new framework, providing Defence with access to the research expertise, infrastructure and developing human capital needed to enhance capability, support economic growth in Australian industry and to encourage future students to consider a career in science, technology, engineering and mathematics.

More information is available at: <https://www.dst.defence.gov.au/partner-with-us/university>

Defence Materials Technology Centre

The Defence Materials Technology Centre facilitates cooperation with Australian industry, research and government agencies to advance technologies in Defence and related sectors in manufacturing engineering and applied science. The Centre aims to strengthen Australian industrial capacity and Defence and national security capabilities.

The Centre operates through a co-investment model applying the funding from Defence or other Commonwealth agencies and leverages additional contributions from industry and research partners. Because of this, the Centre works closely with Defence agencies such as Defence Science and Technology Group and Force Design Division (within Vice Chief of Defence Force Group) to identify Defence capability changes and future needs. The Centre then engages with industry and research partners to find solutions with advancing key technologies.

The Defence Materials Technology Centre focuses on the following capabilities relevant to this Sovereign Industrial Capability Priority:

- New manufacturing technologies
- Performance modelling, simulation and validation
- Design, production and joining of new materials
- Component repair and fabrication technologies
- Robotics and automation technologies
- Repair and life extension technologies
- Prognostics and defect detection capabilities
- Weight reduction, design integration and light weighting materials

Industry Mentoring in Science, Technology, Engineering and Mathematics

Funded under the Australian Government's Industry Growth Centres Initiative, the Graduate Research Industry Partnerships Industry Mentoring Network in Science, Technology, Engineering and Mathematics is an industry-led initiative of the Australian Academy of Technology and Engineering. Industry Mentoring Network in Science, Technology, Engineering and Mathematics facilitates a one year industry mentoring program, connecting PhD students with high level industry leaders (mentors).

The program provides participants one hour of mentoring per month in a professional setting. The Network hosts state-level networking events to broaden the relationships between mentors and mentees across the industry. The Network provides a diverse range of industry professionals the opportunity to engage with academia, share their mentoring skills, and 'give back' to the science, technology, engineering and mathematics community.

This Network provides opportunities for industry and Defence to invest in the science, technology, engineering and mathematics workforce by increasing their understanding of the industry sector and strengthening their skills, as well as enhancing sector collaboration and professional networks.

More information is available at: <https://imnis.org.au/>

Industry 4.0 Initiatives

The Department of Industry, Science, Energy and Resources, in addition to other government agencies and initiatives, have committed to a level of funding to support organisations in pivoting business operations to support the changing manufacturing sector dynamics, particularly around Industry 4.0. The initiatives identified are those perceived to have an impact on this Priority:

- **Higher Apprenticeship Program** up to \$9.2 million committed for industry led alternative apprenticeship training supporting five pilot initiatives. The Industry 4.0 Higher Apprenticeship Program is one of the five initiatives, managed through Skilling Australians Fund, aimed at projected skills requirements for trained technicians. The program model is a traditional paid apprenticeship, with an additional enrolment in an Associate Degree with focus areas in advanced manufacturing processes, automation and robotics, internet of things, cloud computing, advanced algorithms and smart sensors.
- **Investing in science and technology** has \$2.4 billion of investment committed over the next 12 years in Australia's research, science and technology capabilities. Funding includes supercomputers, satellite imagery and leading research in artificial intelligence.
- **Artificial Intelligence and Machine Learning** has \$29.9 million committed under the Taking Local Businesses Global initiative to enable Australian organisations to understand and develop artificial intelligence and machine learning capabilities. Funding extends to project research around these topics and investment in a national ethics framework to outline the standards for adapting to such technology.

Artificial Intelligence (AI) and the Internet of Things (IoT), under the Australian Council of Learned Academies (ACOLA) will be identifying the opportunities, risk and benefits of artificial intelligence, including the associated economic, social, environmental, ethical and cultural impacts that may be presented throughout the development of artificial intelligence technologies over the next decade. This investigation will also determine any associated findings, such as governance needs, education requirements and standards.

More information is available at: <https://www.industry.gov.au/funding-and-incentives/manufacturing/industry-40>

Australian Postgraduate Research (APR) Intern

APR Intern facilitates collaboration between industry and academia by providing a platform for industry to access various PhD disciplines for short-term focused research projects. This provides industry-based training of PhD students, providing industry with highly analytical research expertise to specific projects. APR Intern is the industry arm of the Australian Mathematical Sciences Institute, a collaborative enterprise of Australia's mathematical sciences.

APR Intern currently partner with:

- [New South Wales Defence Innovation Network](#) are investing \$230,000 to place 30 specialist PhDs into internships within New South Wales based defence organisations over three years. This partnership matches New South Wales Defence businesses to high-end expert PhD students from all disciplines.
- [Defence Science Institute](#), providing financial support to businesses servicing the defence sector to support ongoing research challenges.

More information is available at: <https://aprintern.org.au/>



Please direct any questions on the Sovereign Industrial
Capability Priority policy or the information contained in this
Industry Plan to:

defence.icp@defence.gov.au