Australian Government
Department of Defence

SOVEREIGN INDUSTRIAL CAPABILITY PRIORITY INDUSTRY PLAN

Surveillance and intelligence

December 2020


Panasonic

SECRETARY OF DEFENCE AND CHIEF OF THE DEFENCE FORCE FOREWORD

We are pleased to release the *Surveillance and intelligence* Industry Plan, a key deliverable of the *2018 Defence Industrial Capability Plan*.

Persistent and space-based surveillance technologies provide the Australian Defence Force (ADF) and our key alliance partners with situational awareness across multiple domains, including space, and also make broader contributions to national security activities such as border security and counter terrorism. However, surveillance technologies and the data they collect are only as good as the command, control, communications, computers and intelligence (C4I) systems that collate, process, exploit, and disseminate information across the networked Joint Force. As a relatively small military force, the force-multiplier effects provided by surveillance technologies and C4I systems are critical in achieving our objectives to effectively shape, deter, and respond to our changing strategic environment.

We recognise that industry is a key partner in achieving our objectives. This Plan will foster the innovation and collaboration needed to ensure Australia is at the forefront of these capabilities, and that there is agility within the industrial sector to meet the challenges associated with the rapid rate of technological refresh and a dynamic security environment.

Through close consultation with experts from industry and Defence, this Plan identifies the critical industrial capabilities that need to be delivered or supported by Australian industry. Australia seeks access to, or control over, these capabilities to ensure we can meet our future and current needs. This Plan outlines the key enablers of these capabilities, including secure infrastructure and a highly skilled, cleared workforce.

This Plan—which should be read in conjunction with the *Advanced signal processing capabilities* Industry Plan—will guide Defence and industry to develop the capabilities needed to maintain and enhance our industrial base and the warfighting capability of our ADF. The shift of our trusted partners towards an open systems architecture will enable rapid adaptation to new technologies and ensure Australian industry involvement in exporting niche capabilities. To strengthen the ability of our businesses to diversify and encourage increased participation in this sector, this Plan also identifies many of the broader applications of the skills and capabilities underpinning these military technologies.

We would like to express our gratitude to the many contributors who volunteered their time and expertise to support the development of this Plan. We look forward to continuing to build and strengthen our partnership in delivering the products and services needed to support our Defence Force.

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 ten Sovereign Industrial Capability Priorities (Priorities). These Priorities are those that 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 trade-offs associated with sovereign capability. It should be read in conjunction with the Implementation Plan.

Guidance to 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, 19–21).
- 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 the planning and consultation, including preparing for and undertaking market solicitation, such as requests for information (pages 24–33).
- The actions to be taken by government to support development of this Priority (pages 33–36 and consolidated in Annex A).

Guidance to Industry Readers:

This Industry Plan details specific areas of focus for Defence, enabling industry to support growth of 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, the definition of defence sovereignty and what it means to be a Priority (pages 10–11).
- Identification of the critical industrial capabilities and capability enablers related to this Priority and Defence's intent to access or control particular aspects (pages 6, 19–21). This 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 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 24–33).
- Existing support levers available to industry seeking to develop Defence industrial capability (Annex B) (pages 39–45) and the specific actions to be taken by government to support this Priority (pages 33–36).

EXECUTIVE SUMMARY

The dynamic and changing strategic environment requires continual surveillance to collect, analyse, and disseminate large amounts of data that provide situational awareness for the Joint Force. The evolution of the modern battlespace beyond the terrestrial and physical domains into space and global cyberspace adds a further challenge. However, the value of data collected from strategic and tactical sensors is limited and unable to enable situational awareness and facilitate rapid decision making without fusion, processing and dissemination through command, control, communications, computers, and intelligence (C4I) systems across the Joint Force.

Modern warfare is no longer bound by the terrestrial physical domains of air, land and sea, and the ability to sense, understand and control space and cyberspace is becoming critical to warfighting advantage. These trends present both challenges and opportunities for the ADF. A sovereign capability in surveillance and intelligence is critical for Australia to remain at the forefront of this changing environment, enabling the access and control of space, cyberspace, data and information, which ultimately enables the ADF to shape, deter and respond to our strategic environment.

Surveillance and intelligence capabilities—including fixed installations such as the Jindalee Operational Radar Network, integrated undersea surveillance systems, space domain awareness systems and space-based surveillance systems, as well as the C4I systems they feed into—are complex and not readily understood in the broader community. Given the importance of these technologies to the ADF, the Government is seeking to highlight these technologies to ensure businesses with the requisite capabilities have every opportunity to contribute to their development.

The Government recognises the need to foster innovation and collaboration, while also cultivating a skilled digital and systems engineering workforce. This will assure access to, and control over, the critical industrial capabilities outlined in this Plan, and position Australia to rapidly adapt and respond to future challenges. Essential talent in software development and engineering, information technology, data science, mechanical engineering, and electronics and systems engineering will be key to this endeavour. Due to security requirements, there is a need to foster Australian citizens with higher education in these areas, including PhDs. The nature of these skills provides opportunities for businesses in adjacent industries to move into the defence sector; for example, businesses working in cyber security, commercial information and communication technology, and the space industry.

The ADF requires the ability to capture information from a range of strategic and tactical sensors to achieve decision-making superiority in an increasingly contested and congested electromagnetic battlespace. That data must then be rapidly combined and processed into meaningful and actionable intelligence to be shared across the Joint Force and wider national security enterprise to inform military decision-making. This includes sharing information with our key allies and international partners. Networking and integrating data from a range of sensors with joint C4I systems is especially critical for Australia given the force-multiplier effect of this capability coupled with the relatively small size of the ADF.

Recognition of surveillance and intelligence capabilities as a Sovereign Industrial Capability Priority highlights the ever-increasing importance of dominance over the information and cyber domain in modern warfare and the increased reliance on digital technologies that underpin processing, exploitation and dissemination of information. This Plan reinforces the need to maintain Australia's world-leading over-the-horizon radar capability and to build capabilities in the emerging space awareness domain. It also emphasises the importance of C4I integration in the Joint Force and the adoption of Five Eyes interoperability standards to ensure the ADF can exchange information and intelligence with its trusted partners.

Just as information plays an ever-increasing role in operational decision-making, digital technology has become integral to its collection, processing, exploitation and dissemination. Based on software, software-defined hardware, firmware and data, with information and communication technology as critical enablers, these capabilities and technologies are subject to a rapid rate of refresh with life cycles measured in weeks or months.

Related Sovereign Industrial Capability Priorities

This Plan focuses on strategic, national and persistent surveillance technologies, the integration of data from a wide range of strategic and national sensors, and dissemination across the Joint Force. However, it should be read in conjunction with the *Advanced signal processing* Industry Plan, which outlines the tactical sensor and effector technologies that provide real-time data processing and manipulation. The *Advanced signal processing* Plan contributes to the Surveillance and intelligence Priority by feeding critical tactical information into the broader C4I network.

The other closely related Industry Plan is *Enhanced active phased array and passive radar capability*, which focuses on a single sensor technology of critical importance to Defence in which Australian industry has world-leading skills and capability. Advanced radar capability systems are a key component of many surveillance capabilities.

Critical industrial capabilities

Seven critical industrial capabilities underpin this Priority. Australia seeks 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 surveillance and intelligence capabilities are effective and available as needed by the ADF.

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.

HIGH FREQUENCY SENSOR TECHNOLOGIES

Design, develop and sustain active and passive high frequency sensors for long-range persistent air and maritime surveillance, including advanced adaptive algorithms for resilience and assured performance in degraded conditions.

SPACE DOMAIN AWARENESS TECHNOLOGIES

Design, develop and sustain integrated sensor networks for persistent surveillance of space objects and phenomena that can be certified and operated as part of a global network shared with our international partners.

SPACE-BASED SURVEILLANCE TECHNOLOGIES

Design, develop and sustain integrated orbital sensor networks for Earth observation that can be certified and operated as part of a global network shared with our international partners.

BIG DATA PROCESSING AND EXPLOITATION

Design, develop and sustain big data processing and exploitation, dissemination and presentation algorithms and software that enhance operational and intelligence outcomes.

C4I INTEGRATION

Integrate tactical, persistent and space-based surveillance technologies operating at multiple security levels into ADF and Five Eyes command, control, communications, computing and intelligence (C4I) systems.

SECURE COMMUNICATION TECHNOLOGIES

Design, develop, modify and upgrade software and hardware that enables secure communication across the Joint Force.

No single surveillance capability is operationally effective in isolation and must be successfully integrated into C4I systems to allow collected data to feed into broader joint force C4I systems. Defence expects Australian industry to design for interoperability with our trusted partners and support the integration of innovative technologies with other ADF and allied systems. In some instances, there are limitations due to No Foreign Access agreements when employing US-developed software and data. Defence needs the flexibility to dynamically adapt its integrated sensor networks and C4I systems using best-in-breed technologies sourced from both Australian industry and trusted foreign suppliers.

Defence must continuously adapt these technologies and capabilities to meet the evolving security environment and mission requirements. Open systems architecture will facilitate this agility with less need for costly and time-consuming engineering activities. This movement towards open architecture will also provide Australian industry with greater market access and export opportunities for their world-leading innovative technologies and niche or bespoke capabilities. Defence recognises the value of Australian industry innovation in persistent and space-based surveillance systems that may provide the ADF and our allies with unique warfighting advantages.

To ensure Australia retains the identified critical industrial capabilities, the Government seeks to build the following enabling capabilities in partnership with industry 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 surveillance and intelligence 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.

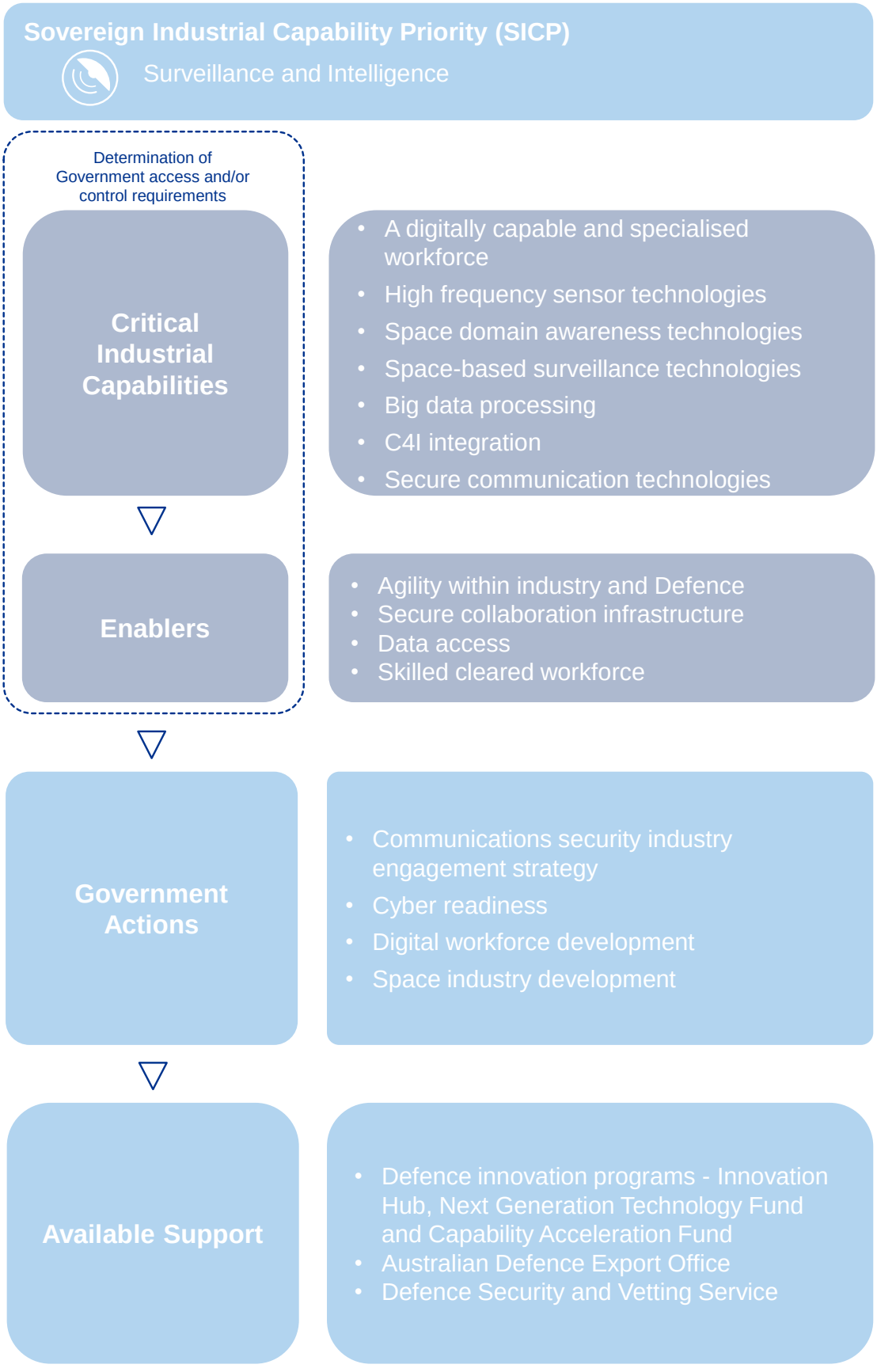
Successful implementation of this Plan

This Industry Plan describes Defence's aspirational priorities for the next three to five years in developing surveillance and intelligence capabilities across many programs and projects in the Integrated Investment Program. Successfully implementing this Plan will create an industrial landscape in 2023–2025 with the following characteristics:

- Defence will continue to operate a world-leading high frequency radar network for regional persistent surveillance and will have progressed towards establishing similar world-leading space domain awareness and space-based surveillance capabilities in partnership with Australian industry.
- Military platforms will begin to benefit from Australian and Five Eyes C4I systems that enhance situational awareness, threat warning, self-protection and targeting using the combined power of all networked surveillance technologies, as well as big data processing (including machine learning, spatial information and other artificial intelligence techniques).
- Australia will contribute surveillance and big data processing technologies to our trusted international partners through exports and government-to-government technology transfers. Australia will be recognised as an innovation leader in these technologies. All Australian-developed technologies and capabilities will comply with international interoperability standards, and Australia will meaningfully contribute to the ongoing evolution of those technical standards.
- Healthy and collaborative relationships between primes, small and medium businesses, universities and Defence, will advance sovereign capability and create competitive advantage for Australian exports.
- Australian industry is continuing to grow 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 Surveillance and intelligence Sovereign Industrial Capability Priority and specific sovereign capability requirements across four key areas. These are standardised across all Industry Plans and are presented in the diagram below and discussed throughout the Industry Plan.



CONTENTS

SECRETARY OF DEFENCE AND CHIEF OF THE DEFENCE FORCE FOREWORD 3
EXECUTIVE SUMMARY 5
CONTENTS 9
STRATEGIC CONTEXT 10
The case for a sovereign industrial base 10
Sovereign Industrial Capability Priority development 11
Policy framework 11
SURVEILLANCE AND INTELLIGENCE 12
Persistent surveillance technologies 14
C4I technologies 16
Capability building blocks 19
Critical Industrial Capabilities 20
Global opportunities 23
Adjacent industries 23
Future evolution 23
CURRENT AUSTRALIAN INDUSTRIAL CAPABILITY 25
Australian industry attributes 26
Value chain 29
National capability overview 30
Workforce and technical skills 30
Industrial processes supporting Sovereign Industrial Capability Priority technologies 31
Assets and infrastructure 33
Risks to domestic industry 33
BUILDING INDUSTRIAL CAPABILITY 36
Industry capability enablers 36
Connecting Defence and the Australian Space Agency 38
ANNEX A. GOVERNMENT ACTIONS 40
ANNEX B. SUPPORT THROUGH INDUSTRY PROGRAMS 41

STRATEGIC CONTEXT

The case for a sovereign industrial base

Sovereign industrial capabilities are considered operationally critical because of the essential strategic advantage they provide 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 needs to 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 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; and
- 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 judges 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] https://www1.defence.gov.au/sites/default/files/2020-08/sicp-factsheet1.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 officially 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:

- 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.

SURVEILLANCE AND INTELLIGENCE

Australian industry must possess an ability to design, develop, maintain, and upgrade persistent and space-based surveillance capabilities so that large amounts of data can be collected, analysed, and disseminated across the Joint Force. This includes developing and upgrading sensors and software, over-the-horizon radar systems, space situational awareness systems, the integration of intelligence and information systems into command, control, communications, computers and intelligence (C4I) networks, high-end integration across platforms, trusted autonomous systems, cryptographic equipment, and weapon systems that provide Defence with improved situational awareness.[2]

To succeed in any battle environment, the ADF needs to know more, and faster, than its adversaries. Surveillance and intelligence data gathering technologies are critical to key systems and platforms within the ADF, and provide the mechanism for the ADF to observe, understand and manipulate the battlespace at the strategic level. Surveillance and intelligence capabilities are essential across the Joint Force and as part of a larger coalition force.

Military commanders rely on information and intelligence to enable operational and strategic decision-making. As the modern battlespace evolves beyond the terrestrial and physical domains into space and global cyberspace, advances in digital technology heighten both the supply and demand for timely and relevant, high-quality data. Achieving decision-making superiority in an increasingly congested and contested electromagnetic battlespace demands enhanced surveillance and intelligence technology integration across the Joint Force and wider national security enterprise.

Historically, surveillance and intelligence capabilities were based on tightly coupled systems-of-systems built with monolithic architectures, closed interfaces and proprietary data formats. Significant engineering effort was necessary to enable limited combinations of specific systems to work together. Until very recently, sensors tended to operate in isolation and the data they generated was stove-piped.

Modern technology now allows for information to be integrated and used much more effectively with less need for costly and time-consuming engineering activities through the use of open systems architectures. This allows Defence to continuously adapt as military missions, threats and operating environments change. Defence also expects this will provide Australian industry with greater market access and export opportunities to Five Eyes and other trusted international partners.

[2] *2018 Defence Industrial Capability Plan.*

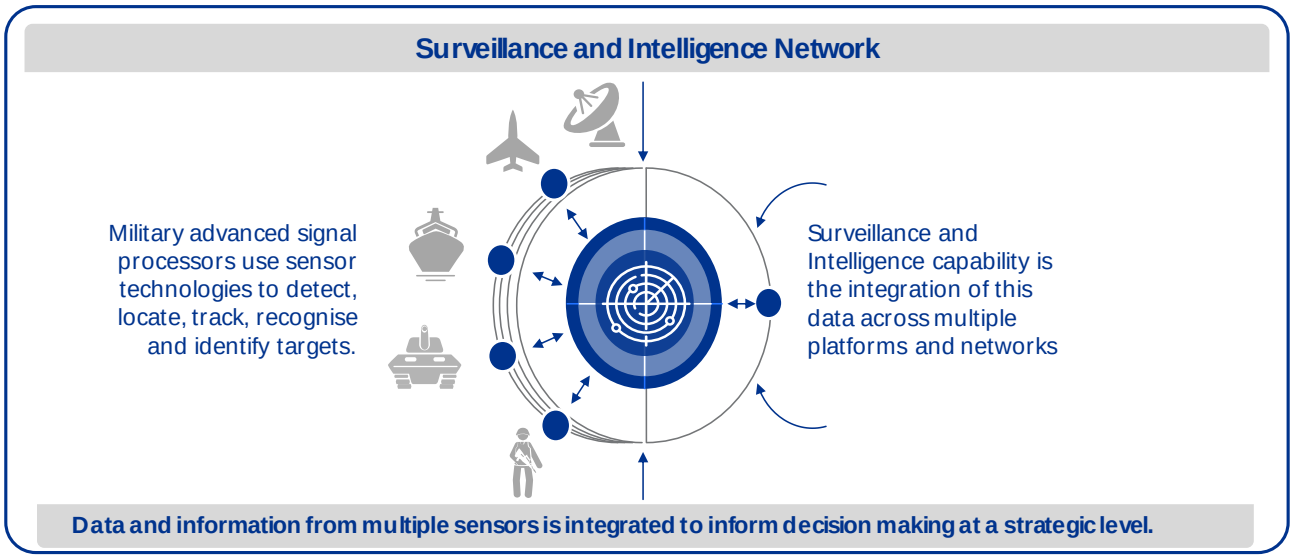


Figure 1: Surveillance and intelligence network

The above figure shows how the tactical sensors described in the *Advanced signal processing* Industry Plan feed into the capabilities identified in this Plan. This Priority focuses on Defence's reliance on a real-time, interconnected network to build a common operational picture. The ADF uses this operational picture to collaboratively plan strikes, re-target weapons platforms while in flight, and work with a multitude of coalition partners. There are two key technologies the ADF uses to integrate information and build the operational picture:

Persistent surveillance technologies are designed to detect, locate, track, recognise and identify targets over broad areas of the Earth or orbital space.

C4I systems are the **Command, Control, Communications, Computers** and **Intelligence** systems used to connect counterpart systems in allied and coalition forces, and trusted international security partners.

Defence currently relies on a range of intelligence capabilities to protect Australia's borders and sovereignty. Persistent and space-based surveillance and C4I systems are sensitive and valuable capabilities for Defence. Applicable technologies are often highly classified and exports may be restricted to a limited number of trusted partner nations. Defence is acquiring these capabilities through a mix of global defence primes, Australian industry providers and in-house development. Australia has world-leading skills and capabilities in this area and this Plan will provide guidance to further grow these into the future.

Recognising these capabilities as a Sovereign Industrial Capability Priority acknowledges the ever-increasing importance of information warfare and its enabling technologies. These technologies play a crucial role in many of the other priorities. Surveillance and intelligence data gathering technologies specific to Defence capabilities serve critical functions and roles for most military platforms and capabilities.

The digital industry

This Priority is different from many others as it is focused primarily on technologies and capabilities within a system, rather than individual platforms. It is supported by a digital industry with most underpinning capabilities based on software, software-defined hardware, firmware and data. This is different to many of the other priorities, which focus on advanced manufacturing processes.

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 the international market. This has been highlighted as particularly important during the COVID-19 pandemic as global supply chains have come under stress.

It features a workforce of data scientists and software engineers who are developing technologies and capabilities with a lifecycle usually measured in weeks or months, not years or decades. This dynamic environment presents opportunities for Australian businesses with the agility and flexibility to meet Defence's changing needs. It also presents challenges for Defence to adapt to more flexible and agile procurement processes.

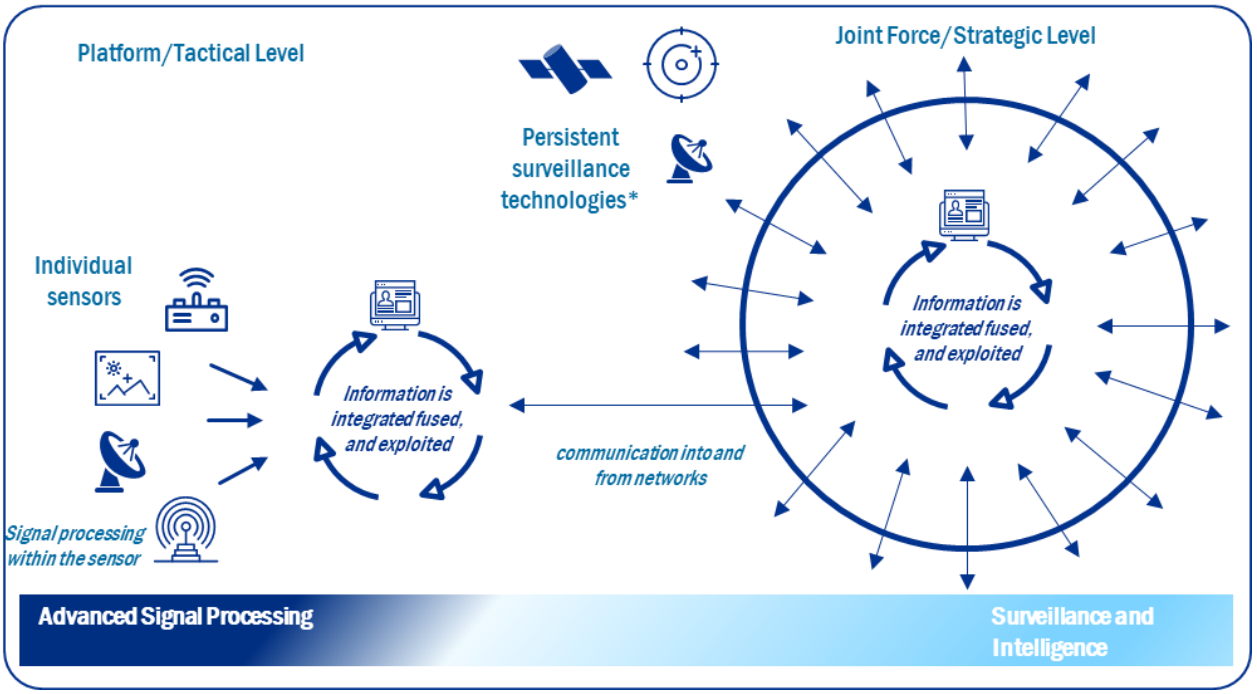


Figure 2: Interaction between the Advanced signal processing and Surveillance and intelligence Priorities.

Persistent and Space-based surveillance sensor technologies

Persistent and space-based surveillance sensor technologies are designed to detect, locate, track, recognise and identify targets over broad areas of the Earth or orbital space.

Persistent surveillance technologies support a variety of Defence capabilities, including global situational awareness, space domain awareness and security, multi-domain strike, and air and missile defence. Persistent surveillance capabilities can also directly contribute to operational and tactical outcomes by providing information to specific force groups and other military missions. Beyond military applications, these capabilities make vital contributions to border security, search and rescue, counter-terrorism, and other multi-agency missions across the broader national security enterprise.

High frequency radar

Radar transmits radio waves then listens for reflected energy from objects such as aircraft and ships. Conventional radars transmit radio waves at microwave frequencies that travel in straight paths and cannot see beyond the horizon. In contrast, high frequency radars transmit waves that travel in curved paths and enable over-the-horizon operation out to hundreds or possibly thousands of kilometres. High frequency radar is highly effective at detecting, locating, and tracking targets with high precision at extremely long ranges. Australia's Jindalee Operational Radar Network is a world-leading high frequency radar.

Space surveillance radar

Space surveillance radars stare upwards at space to monitor satellites and space debris. This technology category includes passive radar, which is a specialised type of radar that does not transmit its own radio waves but instead takes advantage of ambient radiation from third-party radar and radio transmitters.

Space surveillance imaging

Imaging sensors measure the radiation emitted by targets 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. Radar and imaging are complementary technologies, with each used to detect, track and classify targets in different orbits. Space surveillance imaging sensors are ground-based and stare upwards at space to monitor satellites and space debris.

Integrated undersea surveillance systems

Integrated undersea surveillance systems provide persistent coverage over wide expanses of ocean over long periods of time. Systems can be fixed or rapidly and flexibly deployed to areas of interest, and have the capacity to operate in a range of conditions in deep water and shallow littoral environments.

All persistent surveillance sensor technologies share two common characteristics:

- They have the ability to continuously produce massive amounts of raw sensor data that must be processed and exploited to extract valuable information.
- Their sensor apertures are typically distant from their system operators and from the end users of the information they produce.

Integrated undersea surveillance systems

To further safeguard Australia's undersea capability, the *2020 Force Structure Plan* announced over $5 billion of investment for an integrated undersea surveillance system. This includes exploration of optionally crewed or un-crewed surface and undersea systems, an undersea signature management range, and expanded undersea warfare facilities and infrastructure. Defence Science and Technology Group is also exploring undersea surveillance through the STaR Shots program, including advanced sensors and autonomous technologies. These investments will enable fully integrated sensor systems and networks to be developed that provide persistent coverage over wide expanses of ocean and long periods of time.

The critical technologies and industrial capabilities that underpin the individual sensors that make up undersea surveillance systems are captured in the *Advanced signal processing* Industry Plan. The industrial capabilities required to successfully integrate those individual sensors into a broader network, and with the Joint Force, are outlined in the critical industrial capability section of this Plan.

In addition to persistent surveillance technologies, this Plan also covers space-based surveillance capabilities found below. Both persistent and space-based surveillance capabilities are supported by similar industrial capabilities.

Earth observation radar

Earth observation radars on satellites stare downwards at the Earth. These satellites depend on ground station infrastructure to pass data to users. This technology category includes the specialised synthetic aperture radar, which transmits radio waves for long periods of time and integrates reflected energy to synthesise images.

Earth observation imaging

Earth observation imaging sensors on satellites stare downwards at the Earth. These satellites depend on ground station infrastructure to pass data to users. Earth observation imaging is widely used for non-military applications such as Google Maps and other commercial geospatial information services.

Earth observation signals collection

Signals collection systems listen for radio waves transmitted by radars and radio communications systems. Signals collection is highly effective at detecting, locating, tracking, recognising, and identifying targets that transmit radio waves, including most military platforms. Signals collection systems on satellites can observe large regions of the Earth. These satellites also depend on ground station infrastructure.

The infrastructure to transfer, store and process the vast data these capabilities create in remote locations will remain a challenge for Defence as the data requires sophisticated processing and analysis to extract useful information and intelligence products. Analysis is undertaken at an individual capability level—as well as more broadly across multiple capabilities—to meet challenges associated with bandwidth and data storage. Given the role these technologies play in decision making, supporting infrastructure must be secure, highly available and under sovereign control.

While Australian industry has significant capacity in developing certain surveillance capabilities, Australia will retain a level of dependency and partnership with our international partners. The high acquisition value and sustainment costs of surveillance capabilities, particularly those in space, encourages mutual resource sharing with trusted international partners. By contributing to an integrated international network, Australia benefits from the investments made by our partner nations by sharing data

and intelligence products. This includes their investments in space-based sensors, which have global reach and are capable of detecting, locating, tracking, recognising and identifying a broad range of terrestrial objects. As the Australian space sector grows and advances, Defence will seek opportunities for integration of Australian investments into this global network.

The growing importance of space situational awareness to Defence and the broader national security enterprise is driving investment into space domain awareness technologies. Defence looks forward to expanding and networking its space surveillance radar and imaging installations around Australia over the *2020 Force Structure Plan* timeframe. When used together as parts of an integrated sensor network, radar and imaging technologies provide all-weather detection, location, tracking, recognition, and identification capability for space objects above Australia. They are a significant contributor to situational awareness and threat warning information to the Joint Force. The Australian sensor network will be connected to its counterpart networks in the US and other partner nations to enable global space domain awareness extending beyond the areas of space visible from Australia.

C4I technologies

Modern military forces use communications and computing networks extensively to interconnect dispersed command, control and intelligence systems. The ADF fights as a networked joint force and relies on C4I technologies to support decision-making superiority and enable digital data exchange amongst sensors and weapon systems to enhance force lethality and survivability. The force-multiplier effect of C4I technologies offsets the relatively small size of the ADF and represents one of its key warfighting advantages. An integrated joint force contributes directly to our objectives to shape, deter and respond through increased situational awareness, enhanced targeting information and superior decision-making.

For example, the crew of a land combat vehicle equipped with a tactical imaging sensor may not normally interact directly with the air surveillance operators monitoring the Jindalee Operational Radar Network, but both contribute sensor data to the networked joint force and broader national security enterprise. These disparate elements are unified by C4I systems that enable data, information and intelligence to flow throughout the networked Joint Force to the commanders and other consumers. ADF C4I systems connect to counterpart systems in the broader national security enterprise, allied and coalition forces, and other trusted international security partners.

Image 1: Ground based tactical radar sensors contribute to the networked Joint Force

Edge networks

All military platforms in a networked Joint Force need mobile network connectivity. Military edge networks may be based on a combination of commercial and military technologies, such as frequency-agile internet protocol radios and free-space laser links. They must be flexible to support diverse data exchanges between dispersed nodes, ranging from real-time video streams to machine readable data bursts, with encryption options suitable for all security levels from unclassified to top secret.

National networks

The modern battlespace is not constrained to a forward area of operations; it extends into space, global cyberspace, and the national support base. All surveillance technologies rely on facilities in the national support base such as sensor sites, satellite ground station infrastructure, and control centres. All these facilities rely on national critical infrastructure, such as data centres, telecommunications exchanges, and reliable electrical power supply. They need high-capacity, high-availability network connectivity to each other and their offshore counterparts. Defence national networks predominantly use commercial technologies—such as fibre optic cable networks and other carrier-grade network technologies—augmented with military technologies such as high-assurance encryption.

Reach-back links

Military forces deployed to forward areas of operation need resilient reach-back connectivity to the national support base. Reach-back links between military edge networks and Defence national networks are predominantly based on military technologies, such as protected satellite communications and high frequency internet protocol radio, which are supplemented by commercial technologies such as satellite communications and public internet access. There is also potential to augment these commercial technologies with military technologies, such as high-assurance encryption. These links are critical to enable enhanced surveillance and intelligence integration across the national security enterprise.

Cloud computing

The emergence of hyper-scale public cloud computing has made high-capacity data storage and high-power computing accessible to organisations around the world by lowering the cost of entry barriers associated with capital investment in private infrastructure. Cloud computing is widely accepted as a primary driver of digital innovation and is directly responsible for accelerating technological advancement in the digital era. Adapting commercial cloud computing technologies to military and national security use with sensitive and classified data and software is a key enabler of force modernisation and advancements in surveillance and intelligence capabilities.

Edge computing

Military forces deployed to forward areas of operation can benefit from access to cloud computing resources through the reach-back links between military edge networks and Defence national networks. However while those links are resilient, they are not invulnerable and the ADF expects to operate with intermittent and degraded access to national networks during operations in a contested electromagnetic environment. Edge computing technology offers the flexibility of the cloud computing model at significantly smaller scale. It is delivered by computing nodes hosted on military platforms or at forward operating bases in the area of operations, and does not depend on reach-back links. Edge computing enables continuity of military capability—especially sensor fusion and other data processing capabilities—during operations in a contested electromagnetic environment.

Battle management applications

Orchestrating military forces using battle management applications is a principal use of computing in modern warfare. Battle management applications comprise software hosted on computing hardware connected to one or more networks. Battle management applications are typically optimised for warfare in a specific domain. For example:

- an air battle management application is designed to track and visualise a small quantity of fast-moving objects
- a land battle management application is designed to track and visualise a large quantity of slow-moving objects.

A Joint Force must employ and integrate multiple different battle management applications to support multi-domain operations.

Intelligence applications

Another principal use of computing in modern warfare is mining valuable information from data using intelligence applications. These support military action and decision making, and contribute to real-time situational awareness, targeting and threat warning.

Most legacy intelligence applications present raw or semi processed data to human analysts for further exploitation. Modern applications deliver higher-value user experiences—most data processing and exploitation occurs behind the scenes. Analysts focus on insights taken from the information and provide actionable intelligence to support commander decision making.

Intelligence applications are typically optimised for a specific intelligence discipline—such as signals intelligence, geospatial intelligence or human intelligence—but some applications are designed to support all-source intelligence fusion.

The ultimate purpose of surveillance and intelligence capabilities is to support decision making. Given the diversity of sensors operated across Defence, it is necessary to process all the outputs into standardised data formats that can be understood by analytical tools. Big data processing and exploitation are closely related activities to prepare and analyse that data.

- Mathematically powerful techniques such as data fusion are commonly used to 'fuse' or associate disparate sources of information to form the bigger picture.
- Processed sensor data is analysed using statistical methods, machine learning or other artificial intelligence algorithms, and other techniques to extract valuable information.

After data processing, information derived from sensor data needs to be disseminated to decision-makers throughout the Joint Force and broader national security enterprise. The value and relevance of information varies between different users, so matching the right information to the right consumer—and presenting it the right way—is a significant challenge. The challenge will grow as data volumes expand exponentially, and sophisticated presentation and interaction techniques will become increasingly important to optimise user experience.

The diverse sensors employed across Defence, and the C4I systems that integrate these, operate at all security levels, from unclassified to top secret. National security constraints are a significant factor at the secret level and above, and the most highly classified information may be tightly held. It is not technically or economically feasible to operate all systems at the highest security levels at all times. This approach would also compromise Defence missions, such as regional security operations and humanitarian assistance and disaster relief, which require Defence to share information with non-military or non-government organisations that cannot receive classified information.

A multi-level security architecture is essential to enable all sensors and C4I systems to contribute their data, information and intelligence to the networked Joint Force and broader national security enterprise, while maintaining high assurance that sensitive and classified capabilities remain suitably protected.

Future of C4I technologies

Modern C4I technology design practices are embracing open systems architectures. These unify physically diverse communications and computing systems into the ADF edge network, and can move algorithms and software between host systems without extensive re-engineering. Open architectures have significant benefits, but increase the need for ongoing assurance and certification activities to manage the risks of a variable technology baseline. The *Test, evaluation, certification and systems assurance* Industry Plan details the certification and systems assurance required on advanced networks, and complex, software-intensive systems such as C4I technologies.

Open systems architecture

The United States Department of Defense is leading a shift towards open systems architecture within the Five Eyes countries. Key characteristics 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

Interface requirements (including data formats and physical interconnections) are controlled by publishing common guidelines for all suppliers and monitoring compliance.

Interoperability

Components designed and developed by different suppliers can work together properly 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 they can adapt to changing missions, threats and operating environments. Interoperable systems built from modular components can be quickly and easily tested, introduced into service, and continually upgraded and refreshed.

Second, open systems architecture helps promote innovation through increased industry competition, and can improve supply chain resilience by diversifying the industrial base. Defence acknowledges that adaptation to this new commercial approach will take time and present challenges. Defence must provide strong leadership to Australian industry and enforce compliance to interoperability standards to enable success.

Third, Defence expects the open systems architecture approach to be beneficial to those Australian industry entities which embrace a continuous innovation business model. This is especially the case for small and medium businesses with niche or bespoke surveillance and intelligence capabilities that have previously been locked out of global supply chains based on proprietary technologies.

Capability building blocks

Technology alone does not constitute a capability. Sensor technology must be integrated into military platforms and networked across the Joint Force. Assurance of all technology components and their certification for ADF operational deployment is critical to realising full operating capability of these technologies.

The Surveillance and intelligence Priority is built on a set of fundamental capability building blocks, which are shared with the Advanced signal processing Priority:

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

Systems integration and assurance and certification are critical to sovereign industrial capability. These building blocks enable Australian and foreign technologies from multiple vendors to be integrated into ADF C4I systems. However, assurance and certification is not a focus area in this Sovereign Industry Capability Priority, as it is covered extensively in the *Test, evaluation, certification and systems assurance* Industry Plan.

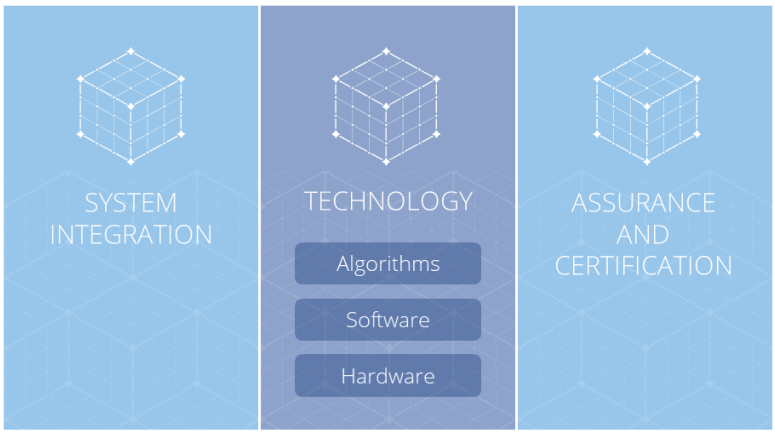


Figure 3: Capability building blocks

These capability building blocks apply to all stages of the value chain. Systems integration, and assurance and certification activities are predominantly performed during the later stages of the value chain, from research and development to disposal. They are also essential design and manufacture considerations from the earliest inception of a new capability.

Critical industrial capabilities

Critical industrial capabilities underpin the Sovereign Industrial Capability Priorities. They are Priority-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.

Defence relies on Australian industry to provide ongoing support and sustainment to surveillance and intelligence capabilities. This includes maintaining their operational effectiveness and suitability against rapidly evolving threats through updates and upgrades. Australian industry providers of these capabilities must maintain suitable security credentials and export permits to support the ADF and trusted international partners.

Defence has identified seven critical industrial capabilities for this Priority. These underpin the ability to leverage current, emerging and disruptive technologies into ADF surveillance and C4I systems.

1

A DIGITALLY-CAPABLE AND SPECIALISED ENGINEERING 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 electrical and systems engineering.

Platforms and technologies that deliver surveillance and intelligence will continue to be replaced and upgraded. Rather than an emphasis on platforms, these capabilities are flexible and agile, driven by a highly skilled Australian workforce with essential talent in software development and engineering, information technology, data science, electronics, microelectronics, communications and systems engineering. These skills directly contribute to each of the other critical industrial capabilities in this Plan. Australian industry must be capable of designing, upgrading and enhancing the performance of ADF surveillance technologies, and integrating these into C4I systems across the national security enterprise. The development and growth of these skills in Australia is critical to deliver this Priority.

2

HIGH FREQUENCY SENSOR TECHNOLOGIES

Design, develop, update and upgrade active and passive radio sensors for long-range persistent air and maritime surveillance, including advanced adaptive algorithms for resilience and assured performance in degraded conditions.

Australian industry must be capable of supporting the Jindalee Operational Radar Network and maintaining its world-leading capabilities. This will be achieved by creating advanced adaptive algorithms for high frequency radar digital signal processing.

Our potential adversaries recognise the significant contribution made by the Jindalee Operational Radar Network to Defence capability, and may seek to degrade its performance through electronic attack, or other means, in a time of conflict. Advanced adaptive algorithms that enable resilient and assured performance in degraded conditions are therefore critically important to this capability.

Jindalee Operational Radar Network

The Jindalee Operational Radar Network is an Australian high frequency sensor that can monitor air and sea movements to the north of the continent at very long ranges. It represents current world-leading capability in high frequency sensor technology and contributes significantly to situational awareness and threat warning information for the Joint Force.

The Jindalee Operational Radar Network is a fully sovereign, integrated, assured and certified Australian system. It is a key example of Australian developed innovation and is currently undergoing a major upgrade project that will enable continuous capability assurance into the future through digital signal processing upgrades.

SPACE DOMAIN AWARENESS TECHNOLOGIES

Design, develop and sustain integrated ground-based space surveillance sensor networks for persistent observation of space objects and phenomena that can be certified and operated in a contested environment as part of a global network shared with our international partners.

Australian industry must be capable of supporting Defence's emerging space domain awareness capability by:

- creating space surveillance sensors, and networking and integrating these with mission control systems; and
- assuring and certifying the Australian space domain awareness capability to connect to counterparts in the United States and other partner nations.

Australian industry already has world-leading capability in imaging and passive radar space surveillance capabilities, and these advanced sensors must now be integrated into a sovereign space domain awareness capability that is interoperable with, and connected to, counterpart systems in the US and other partner nations.

Assured access to the space domain is essential in modern warfare and is critical to maintaining ADF warfighting advantages. Defence relies on space for position, navigation and timing, global communication and intelligence, surveillance and reconnaissance. Ground-based sensors that provide comprehensive space domain awareness are a fundamental prerequisite to space control.

SPACE-BASED SURVEILLANCE TECHNOLOGIES

Design, develop and sustain integrated orbital sensor networks for Earth observation, that can be certified and operated as part of a global network shared with our international partners

Australian industry must be capable of supporting Defence's future space-based surveillance capability by creating orbital Earth observation sensors, networking and integrating those sensors with mission control systems, and assuring and certifying the Australian space-based surveillance capability to connect to counterparts in the United States and other partner nations. This includes the ability to move and reposition sensors as required.

Australian industry already has world-leading capability in many tactical sensor and sensor fusion technologies—as described in the *Advanced signal processing* Industry Plan—which could be adapted to the unique environmental constraints of space to enhance Defence's earth observation capabilities.

Sensing from space offers many warfighting advantages, including increased operational up time, and reduced risk to life and equipment compared to deploying tactical sensors forward into the battlespace on military platforms. These advantages come at the cost of building spacecraft and launch vehicles, hardening systems to survive in space, maintaining spacecraft in orbit and earth-to-orbit secure communication links, and the challenges associated with operating within an increasingly congested and contested space domain. Defence does not anticipate a requirement for space launch associated with this capability in the next three to five years, and it is not presently included in scope for this critical industrial capability.

5 BIG DATA PROCESSING, EXPLOITATION AND DISSEMINATION

Design, develop and sustain big data processing, exploitation, dissemination and presentation algorithms and software that enhance operational and intelligence outcomes.

Australian industry must be capable of enhancing ADF decision-making superiority in a dynamic and multi-domain battlespace through creating innovative and advanced big data processing, exploitation, dissemination and presentation algorithms, and software for battle management and information systems. Many ADF battle management and information systems are based on foreign hardware and software. Defence requires Australian industry to interface its data processing algorithms and software into these foreign systems. Modifications to existing hardware designs will also be required to satisfy the unique operational requirements of the ADF and suit the environmental characteristics of the operating environment.

Big data processing and exploitation are essential in achieving information superiority at the strategic level. This is particularly critical in a complex modern battlespace that extends beyond the terrestrial physical domains into space and global cyberspace. Surveillance data from all of these domains will require a strong spatial industry when managing data to enable an effective surveillance capability. Data from all sources—including ADF and allied surveillance systems, all intelligence disciplines, and open source and commercial data providers—must be collected, processed, exploited, securely stored and protected, and then rapidly and reliably disseminated to all decision makers throughout the networked Joint Force and broader national security enterprise. As data volumes grow exponentially, sophisticated presentation and interaction techniques are becoming increasingly necessary to optimise the tactical user experience and allow warfighters to focus on their mission, not data manipulation.

Spatial information:

Spatial information is a broad term for referring to the skills, data and technologies used to create, analyse, manage, interpret and connect information about the position, area and size of objects within reference to time.

Spatial analysis uses various analytical tools, techniques and procedures to manipulate big data sources and provide efficiency in data analysis processes. Spatial analysis processes raw data to ensure Defence practitioners are aware of the context surrounding the information presented to them.

Australian technology in the management of big space-derived spatial data is world-leading (for example, Geoscience Australia's Digital Earth Australia[3]) and supported by a diverse and dynamic local industry.

6 C4I INTEGRATION

Integrate tactical persistent, and space-based surveillance technologies operating at multiple security levels into ADF and Five Eyes command, control, communications, computers and intelligence (C4I) systems.

Australian industry must be capable of integrating ADF tactical, persistent and space-based surveillance systems, battle management, and information systems operating at multiple security classifications into a cohesive C4I system. This will be done through a combination of system, network, and data integration activities to interconnect diverse and dispersed ADF systems, and through assurance and certification of these interconnected systems for operational use by the ADF. Defence expects Australian industry to design technologies for ADF C4I integration and Five Eyes interoperability, including conforming with standards such as Joint Interface Control Document 4.2.

Australian industry must also be capable of adapting foreign technologies for ADF C4I integration. The ADF depends on its battle management and intelligence systems – which are interconnected with its surveillance systems through a variety of edge and national networks – for situational awareness, targeting, and threat warning.

A multi-level security architecture is essential to enable all sensors and C4I systems to contribute their data, information and intelligence to the networked Joint Force and broader national security enterprise. This must be done at the lowest allowable security classification while maintaining high assurance that sensitive and classified capabilities remain suitably protected.

[3] http://www.ga.gov.au/dea

SECURE COMMUNICATION TECHNOLOGIES

Design, develop, modify, and upgrade software and hardware that enables secure communication across the Joint Force.

Reliable secure communications are essential to most modern military capabilities. They enable sensors, platforms and people to share information with others that need it. Defence's communications are already under substantial threat. Adversaries seek to identify, intercept and disrupt our communications to understand our plans, degrade our situational awareness, and undermine command and control, ultimately eroding our ability to fight and win.

State-of-the-art sovereign communications security technologies that harness the most up-to-date technologies and techniques will ensure information reaches authorised recipients at the right place and time, and in the form intended, without undermining other aspects of security. Communications security affords flexible protection commensurate with the sensitivity of the information. There are increasing opportunities for Australian industry to support Defence's communications security requirements. These opportunities will be constantly reviewed by Defence, in consultation with the Australian Signals Directorate, to ensure that the Commonwealth provides updated guidelines to support Australian industry.

Australian industry must have the ability to develop software-based solutions to ensure that military platforms can securely communicate with other platforms and across the Joint Force. A key component of industry solutions is the ability to update and upgrade secure communications technologies to account for the changing threats, done primarily through software development and engineering capability. Recognising Australia has alliance partners and operates as part of a Joint Force, Australian industry also needs to be able to deliver communication security capabilities that are compatible and interoperable with our alliance partners.

Global opportunities

This Priority offers meaningful export opportunities to Australian industry, where innovation in surveillance and big data processing technologies can be exported to Five Eyes and other trusted international partner nations. Australian industry will need to adopt and contribute to advancing 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 in and developing these critical industrial capabilities will provide important capability for Defence and enable global opportunities for Australian industry.

Adjacent industries

The Surveillance and intelligence Priority provides opportunities for businesses in adjacent industries, such as spatial data management, cyber security, the space industry, and commercial information and communication technology, with the requisite skills to move into the Defence sector. Companies seeking to move into the Defence sector must ensure they meet Defence security requirements and have an appropriately cleared workforce.

Future evolution

Defence expects continuous growth of these surveillance technologies for the foreseeable future. In the digital era, there are numerous innovative commercial technologies that could have valuable military applications or disrupt established military capabilities. Most of these technologies are software-defined and will rapidly progress through multiple generations in the time it takes Defence to acquire and field a new major platform, such as a ship, submarine, combat vehicle or aircraft. Australian industry must be prepared to respond to emerging and disruptive technologies to support the ADF.

Defence expects the next significant evolution in integrated C4I capability will be a widespread shift from national networks and cloud computing to edge networks and edge computing. The ADF currently relies on support back from its forward deployed force elements to its national networks, and cloud computing resources to enable force-level C4I integration. Defence recognises the limitations with this approach, and mitigates against these by pushing data processing and exploitation closer to the point of data collection, to the tactical sensors integrated onto military platforms. Defence also expects C4I integration to become less dependent on complex systems integration and more focused on data standardisation.

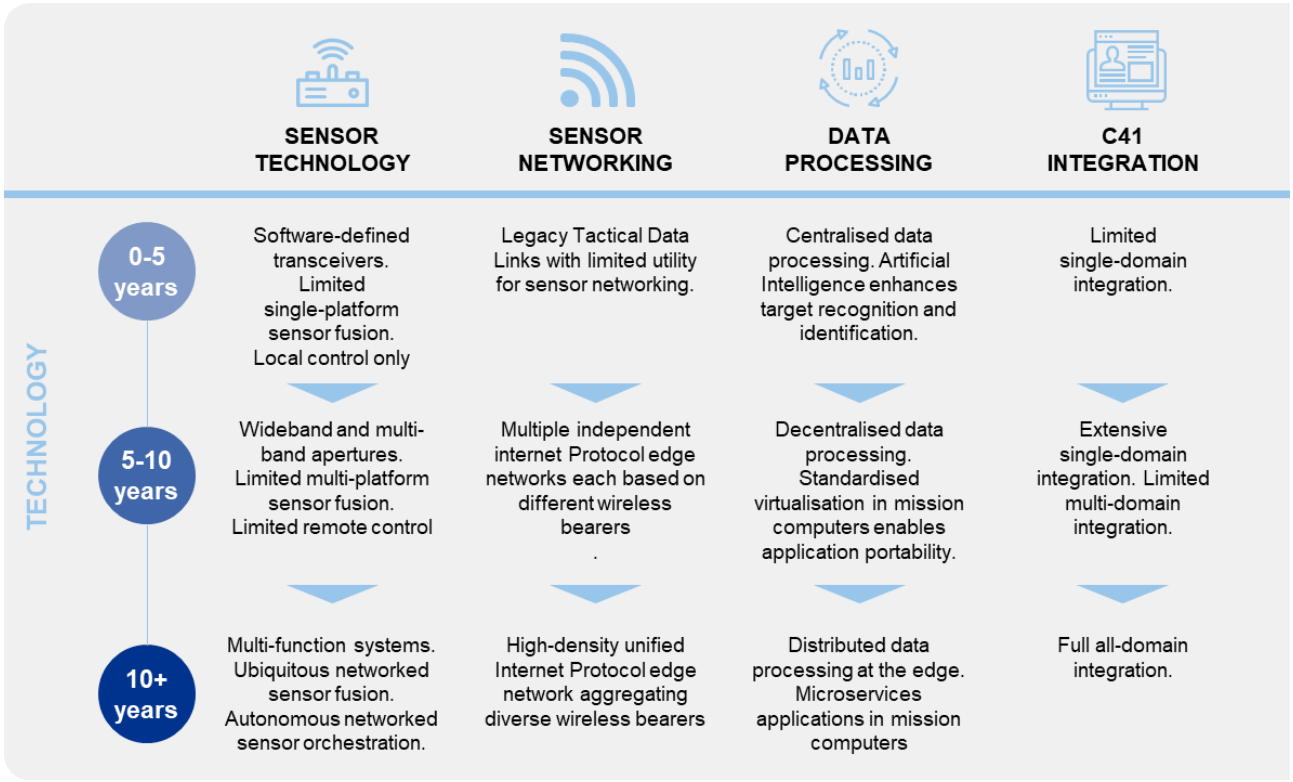
The maturation of event-based intelligence systems through machine learning techniques will support a shift towards edge computing and networking. For example, a military surveillance mission to find a specific ship at sea may require several hours of video to be recorded to extract a single image of the target. The legacy approach to surveillance and intelligence would transport, store and process all the data, while an event-based approach would only transport, store, and process the much smaller amount of data representing the target image. However, machine learning and other artificial intelligence techniques

are required to enable edge computing close to the sensors to identify and isolate the valuable data without human participation. Reducing the amount of data that must be transported across edge networks and reach-back links will improve C4I system performance and resilience in a contested electromagnetic environment.

Defence will require significant automation of data processing, exploitation, and dissemination to support investments in tactical, persistent and space-based sensors. Human cognitive capacity is a valuable and limited resource, best applied to deriving meaningful and actionable insights from information, and should not be wasted on extracting information from, or manipulating, raw data. Industry must deliver machine learning and other artificial intelligence techniques to automate data processing, exploitation, and dissemination activities, and enable personnel to focus on building actionable intelligence to support decision making. These technologies will also enable Defence to operate more sensors without a significant expansion of its workforce.

A shift towards an open systems architecture approach will enable new surveillance and C4I technologies to be rapidly adopted by the ADF with less need for costly and time-consuming engineering activities. This will enable Defence to continue evolving its systems architecture and maintain warfighting advantages as missions, threats and operating environments change. This will provide Australian industry with greater market access and export opportunities.

The following graphic summarises key trends in sensor technology, sensor networking, data processing and C4I integration that will influence this Priority, and the closely related Advanced signal processing Priority over the next decade.



CURRENT AUSTRALIAN INDUSTRIAL CAPABILITY

Advanced signal processing and Surveillance and intelligence are two Sovereign Industrial Capability Priorities served by a single 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 industry is digitally focused on technology that is continuously and rapidly evolving, and so industry must be agile and innovative to keep pace. Australia has an emerging industrial capability to support Advanced signal processing and Surveillance and intelligence, including some world-leading research and development in signal processing for imaging, sonar and passive radar. Organisations vary greatly in size from micro-businesses to large international primes, and their approach to research, development, and delivery of products and services varies greatly across the sector.

The Defence value chain presents 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 understand the strengths and weaknesses of the domestic industry, as well as to determine if action is needed to ensure that Defence has the access or control it needs in relation to this priority.

Manufacturing advanced electronic components in Australia for military applications is unlikely to be economically viable because there is limited ADF demand for these components. Australia, as the place of hardware manufacturing, is not a prerequisite or requirement for this Sovereign Industrial Capability Priority. What is important is the capability to design and develop system hardware, firmware, software tools, and algorithms in Australia. Access to and protection of, intellectual property is key to this industry and is vested in its highly educated and technically skilled workforce. Security is also 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 Surveillance and intelligence and Advanced signal processing Priorities. Attributes and features that are unique to the surveillance and intelligence industry are highlighted with the following symbol:

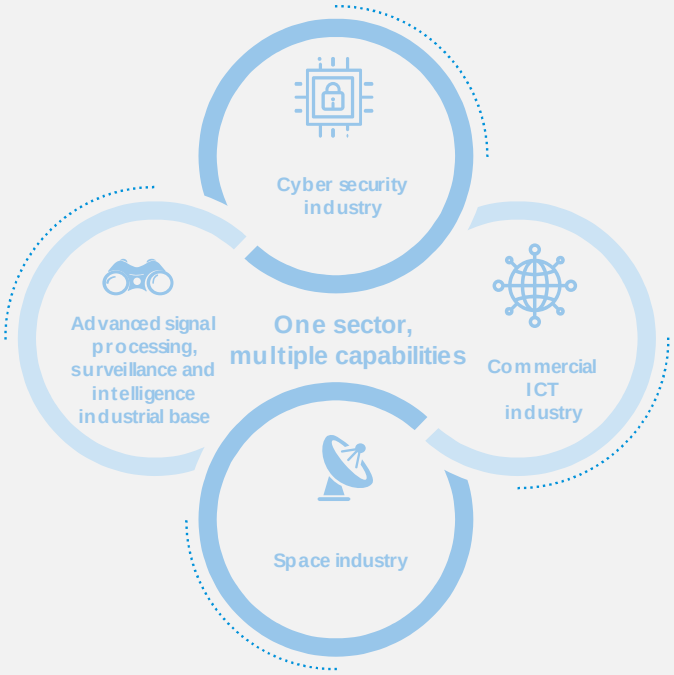
Australian industry attributes

Findings from extensive consultation undertaken during the development of this Plan—as well as research and analysis into the composition and characteristics of Australia's industrial base—provides insight into the attributes of the current Australian industry capability. The breakdown of Australia's surveillance and intelligence industry in this section is based on data gathered during industry consultations across all Sovereign Industrial Capability Priority Industry Plans to date, covering 141 organisations, plus the 40 engaged directly for these priorities.

One sector, multiple capabilities

The Surveillance and intelligence and Advanced signal processing Priorities are supported by a shared industrial base. While Defence's individual capabilities 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.

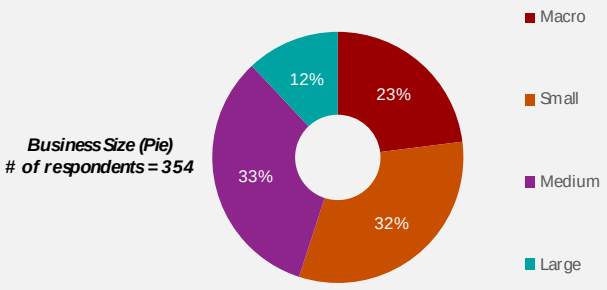
This overlap and commonality among the industries brings both strengths and challenges for the sector. The knowledge and capability in commercial industries can be leveraged to advance defence industry capability, but this also brings significant competition when it comes to hiring and retaining the right people. There are other major customers within the Australian Government competing for the same resources as Defence. In particular, the commercial ICT, spatial, cyber security and space industries in Australia all have a healthy pipeline of work. Through consultations, it was revealed that many organisations in defence industry are also servicing national security clients, often with more ease and agility than Defence procurement allows.



Size and composition

The majority of respondents to the survey who indicated an ability to support this Priority are small and medium-sized enterprises,[4] 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 in 2018.[5] While the collection process for the Centre's data is subject to the respondent's interpretation, it provides an industry snapshot of contributors to the 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 the current Australian industry capability.



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

[4] The survey categorises organisations as micro (up to four employees), small (five to 19 employees), medium (20 – 200 employees) and large (200+ employees).
[5] 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, not validated through other sources; accordingly there are limitations in terms of data bias and representation of the sector.

A digital workforce

In many ways this sector resembles the commercial digital industry sector, which tends to have a greater focus on manufacturing. This sector 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. 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 that spends years specialising in radar would require years more study to later 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 in the commercial digital industry, working on Defence projects 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 provide higher rates of remuneration.

While commercial technologies are often adaptable to Defence needs, innovation within this sector can rarely be adapted to commercial applications and markets. 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 talent pool.

Defence expects greater industry investment in the critical capabilities that underpin this Priority will deliver benefits to the broader economy. Greater capability in data science and software engineering will help place Australia at the forefront of the global technological revolution, and create innovation in other sectors of the economy.

Sustaining this specialised and valuable digital workforce requires continuous investment by Defence in industry research, and development to bridge the gaps between Defence projects. Any interruptions to Defence investment inevitably leads to 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 keep up with this rapid rate of change.

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

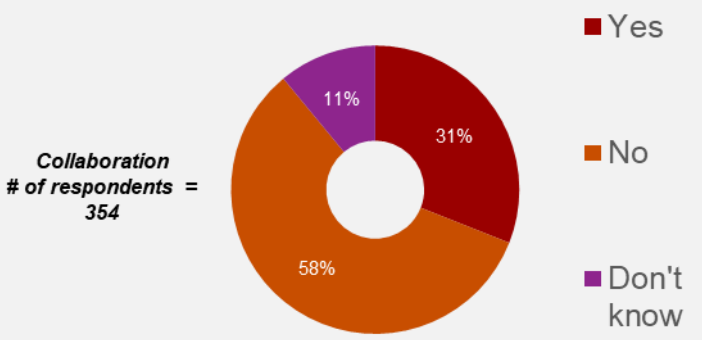
Defence is working with industry to improve the pull-through of industry research and development breakthroughs into operational capability for the ADF. Innovation funding from the Next Generation Technology Fund and Defence Innovation Hub are promoting research and development, and the recently announced Capability Acceleration Fund will invest over $130 million from the middle of this decade to support disruptive technology developments 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 vary price point and quality in an attempt to increase market share.

Collaboration

Industry data demonstrates that while collaboration does occur, there are opportunities to increase this in the sector.

This industry has complex and niche capabilities that would benefit greatly from more cooperation. Increased research and development collaboration could advance sovereign technology. Current Defence procurement drives single prime-multiple sub-engagement which promotes risk transference rather than risk sharing. Intellectual property ownership, licencing and protection issues force a lot of unnecessary duplication of effort within industry.



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

Emerging modular architectures based on open standards can enable a new generation of 'best-of-breed' capabilities to be built from algorithms, software and hardware sourced from different vendors. This technology trend represents a significant opportunity for Australian defence industry—especially innovative and agile small businesses—to contribute to the advanced signal processing and surveillance and intelligence capabilities across the marketplaces for our partners.

Primes recognise the valuable contributions small and medium sized 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, development facilities and specialised test and evaluation infrastructure available to their smaller partners at low or no cost.

Global sector dynamics

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

The Australian Government uses the United States Government's Foreign Military Sales to procure capabilities such as aircraft and high-end combat management systems. Australian industry access to intellectual property is an ongoing challenge to combining 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 with less peaks and troughs in demand in comparison to other markets and customers.

Manufacturing quantities required by the ADF are often too small to justify investment in automation and production. Many Australian businesses therefore rely on offshore manufacturing of their designs 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 alternatives. 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. Some sovereign industrial capabilities are necessary to prototype and manufacture limited quantities of hardware. It is also important that sovereign capability is maintained to tailor foreign hardware to suit Australian conditions.

Industry consultation

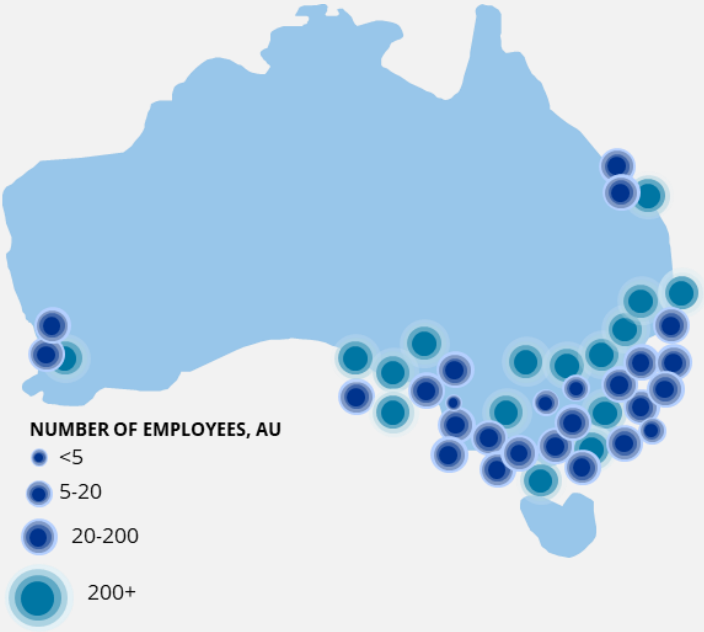
We met with industry, academia and associations representing all parts of the value chain and the full suite of critical industrial capabilities

141 ORGANISATIONS ENGAGED INDIRECTLY VIA OTHER PRIORITIES*

40 ORGANISATIONS ENGAGED As of 12/03/2020

ORGANISATION FOCUS

5	19	30	20
FRIMES	SMEs	SOFTWARE	HARDWARE



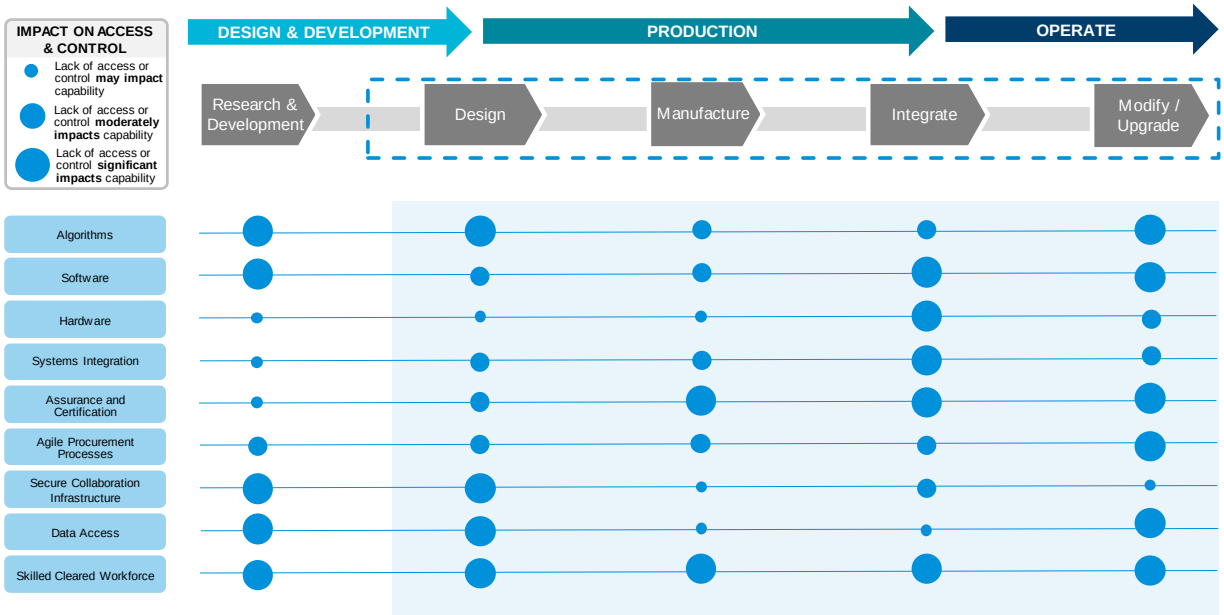
NOTE: Organisations with various locations in Australia have been mapped to their primary location relating to this SICP

* 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 presents the activities involved in designing, developing, producing and implementing through life support of the capabilities defined within this Priority. In comparison to other Sovereign Industrial Capability Priorities, Surveillance and Intelligence has 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.

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).



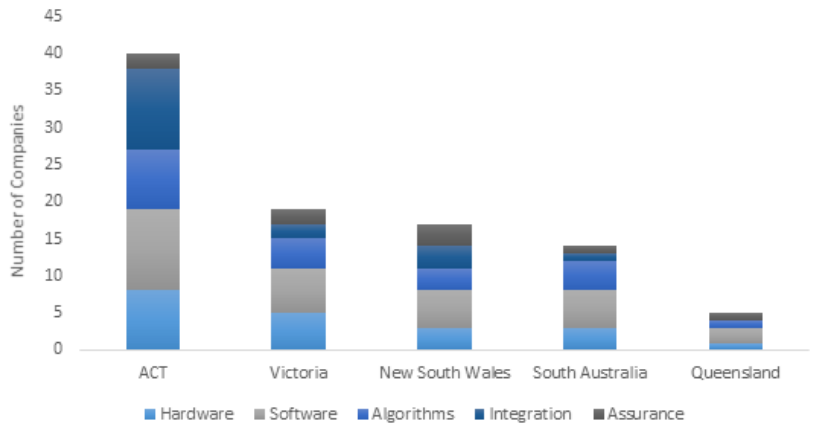
Value chain analysis of this industry sector identified strengths in research and development, software development and systems and platform integration, which align to the needs of this Priority.

National capability overview

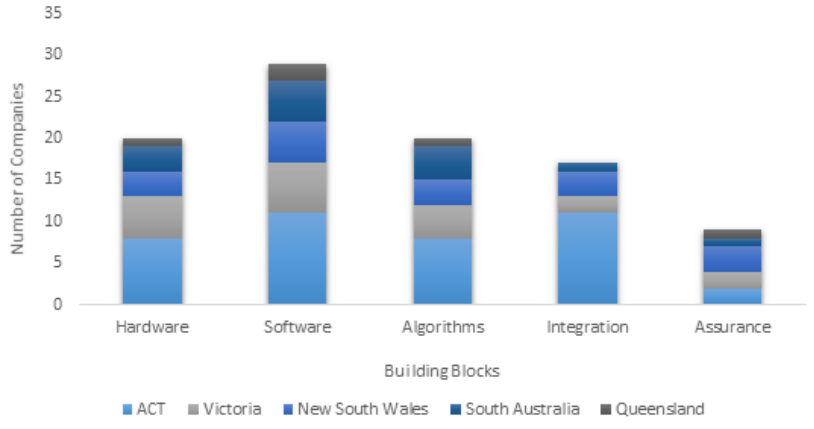
The chart below shows the composition of Australia's advanced signal processing—and surveillance and intelligence industrial capability—based on data gathered during industry consultations. Given the sensitive and niche nature of this work, the companies involved in this sector work almost exclusively in the defence industry.

Numerous insights have been derived through industry engagement in developing 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 buildings 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 at least have their head office functions located in close proximity to government agencies, as well as the disproportionately high number of ex-Defence personnel who are typically employed in defence industry and live in Canberra.

Software is shown to be the most represented building block across all states, while hardware and algorithms were equally the second most featured building block. Assurance work featured the least, which may be a result 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 reveals the composition of companies in this sector. For example, many companies that 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 the largest industrial base in Australia's south-east states.



Software development is a critical capability building block for this sovereign capability, and the breakdown of industry is reflective of 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 and compete with a global commercial digital industry for talent. Essential talent in software development and engineering, information technology, data science and mechanical, electronics or other specialist engineering—especially at the PhD level—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, more often requiring years of significant investment in postgraduate studies and on-the-job training.

An understanding of the Defence environment and the requirements of the systems and platforms is also paramount to the success of this industry. This is why defence industry frequently hires ex-military personnel or Australian Public Service employees across various positions to bring the required level of expertise. However Defence does not internally cultivate a digital workforce with the skills needed by this sector, so it struggles to find the right human resources in Australia to fulfil these roles. Engineering within Defence is predominantly administrative and not oriented towards digital technologies, so there is no healthy Defence to industry pipeline like those that exist for other sovereign industrial capabilities.

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. Further, a notable proportion of graduates from Australian universities with the digital skills needed by this sector are international students who are not able to hold an Australian security clearance.

Industrial processes supporting Sovereign Industrial Capability Priority technologies

A sovereign capability of surveillance and intelligence is not dependent on the ability to build hardware. Instead it requires the ability to integrate systems and develop software and algorithms to run within this hardware.

Software development

Surveillance and intelligence capability is driven by:

- firmware;
- software and software-defined hardware; and
- data.

Sovereignty is derived from the ability to adapt systems, especially in software, to suit the specific needs of the ADF. This could include integrating foreign and domestic technologies.

It is critical that Australian industry support Defence with tailored solutions, unique software and algorithms, and that these can be tested, modified, maintained and upgraded on an ongoing basis.

System integration

Surveillance systems do not exist or operate in isolation. To provide useful and meaningful data to Defence, sensors must be integrated with military platforms and all systems across all platforms must be integrated with the ADF C4I enterprise. System-level performance can be enhanced through signal processing, but force-level capability depends on C4I enterprise integration. The surveillance capabilities described in this Plan, along with the diverse array of tactical sensor capabilities employed by the ADF, generate vast amounts of data that must be integrated with C4I systems to extract valuable information for Defence and the broader national security enterprise.

Developing and growing system integration skills within Australia is critical for this Priority, especially with increasing commonality in systems across military platforms. While the ADF operates many foreign systems and platforms, it has unique requirements and operates its own unique C4I enterprise. It is critical therefore, that Australian industry can effectively integrate surveillance and intelligence capabilities, with the related capabilities outlined in the Advanced signal processing Industry Plan.

The correct commercial arrangements between Government and industry will create agile systems integration capability in Australia. Defence is already adopting this approach on combat system integration through a Defence Industry Collaboration Deed with ASC Shipbuilding, Saab Australia and Lockheed Martin Australia.

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 digital industry best practice, and are also motivated by the growing need of militaries to rapidly recompose their 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 as soon as possible to ensure their innovations remain operable by Defence 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.

Space domain awareness

The ever-increasing importance of space to military operations is driving investment in new space domain awareness.

Australian industry supports Defence's emerging space domain awareness capability by:

- creating space surveillance sensors;
- networking and integrating these with mission control systems; and
- assuring and certifying the Australian space domain awareness capability.

Australian industry already has world-leading capability in optical and passive radar space surveillance sensor technologies. These advanced sensors must be integrated into a sovereign space domain awareness capability that is interoperable with, and connected, to counterpart systems in the United States and other partner nations. Assured access to space capabilities is essential in modern warfare and critical to maintaining ADF warfighting advantage. Defence relies on space for position, navigation and timing, global communication and intelligence, surveillance and reconnaissance. Comprehensive space domain awareness and the ability to deliver this to the ADF is therefore a fundamental industrial proficiency for this capability.

CASE STUDY

EOS Space Systems

For over 30 years EOS Space Systems has been developing and facilitating leading-edge space technology in Australia. By developing a multi-technology (passive optical, active optical and thermal sensors) and multi-site approach (Mt Stromlo, ACT and Learmonth, WA), EOS Space Systems has developed unique Australian capabilities in acquiring, identifying and tracking space objects. This includes the world's only autonomous laser network capable of tracking an object the size of an Australian one dollar coin at one thousand kilometres above the earth's surface.

EOS Space Systems is supporting Australia's contribution to global space surveillance networks by supplying this highly accurate space situational awareness data to minimise the risk of space collisions to active spacecraft and launch vehicles. As space becomes ever more competitive, contested and congested, EOS Space Systems' capabilities will be essential to protecting Australia's national assets.

Since 2016, Defence has contracted EOS Space Systems to provide space domain awareness data, providing world-leading performance and remotely commanded autonomous Satellite Laser Ranging Systems which can:

- track very small space debris objects with high accuracy;
- complete high precision orbit determinations; and
- conduct real-time collision warnings for satellite owners.

The technology can be integrated with the United States Air Force Space Situational Awareness network, supporting interoperability with our allies and contributing valuable intelligence to our integrated C4I enterprise.

Assurance and certification

Assurance of all technology components and their certification for ADF operational employment is critical to realising capability from technology. The ability to achieve high levels of assurance and meet the required certification standards is critical to this capability as most system hardware will likely continue to be manufactured overseas. It is acceptable to have a mission critical system that includes foreign technology components, as long as Australia has control of its certification, integration and ongoing assurance.

This Priority relies on:

- the ability to ensure the appropriate level of control over foreign hardware and platforms; and
- ensuring they can operate in the unique Australian environment, achieving certain performance criteria within a determined risk tolerance.

The assurance and certification capability:

The *Test, evaluation, certification and systems assurance* Industry Plan will set out the requirements for assurance and certification of technology to support sovereign surveillance and intelligence capabilities. This includes cyber worthiness and integration into an effective Joint Force. These activities are recognised as a key building block for the Surveillance and intelligence Priority.

While this is achievable for foreign manufactured hardware, it is very difficult to reach the same level of assurance with foreign developed software without access to source code, which is why it is important to retain the software development capability onshore.

Assets and infrastructure

Surveillance and intelligence capability depends on fixed sensor sites, remote operations centres and satellite ground stations around Australia. Many of these facilities are located in remote environments. They depend on reliable and resilient network connectivity to high-capacity computing and data storage infrastructure. Australian control over this national critical infrastructure is essential to deliver a sovereign surveillance and intelligence capability.

While Defence operates its own private networks and data centres, it also depends significantly on access to commercial public networks, data centres and cloud providers to enable these capabilities. Australian ownership and control of telecommunications network infrastructure is an essential security layer for protecting sensitive and classified data-in-transit between facilities around Australia. Likewise, Australian owned and controlled onshore data centres (including cloud data centres) are an essential security layer for protecting data-at-rest. System administration of network, computing and storage infrastructure by Australian nationals in onshore locations is also critical to protecting Defence's sensitive and valuable surveillance and intelligence 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 economics of scale must be addressed to achieve long-term success in this industry.

Access to test infrastructure

A critical component to developing advanced signal processing, and surveillance and intelligence capabilities, is access to:

- specialised test infrastructure for testing sensor functionality; and
- Defence Secret Network test enclaves for testing integration of sensors to C4I systems.

Access to secure facilities and information and communications technology

Research and development of sensitive technologies often must be conducted in accredited secure facilities using accredited secure information and communications technology. Accreditation can take over two years and cost hundreds of thousands of dollars. This deters new businesses from entering the defence industry, which is a significant barrier to the growth of surveillance and intelligence capabilities in Australia. Industry needs to consider working to develop joint-user facilities with secure cyber environments to develop, test and modify their sensitive software and technologies.

Access to the right skills

The workforce in this industry requires tertiary education in relevant technical disciplines. A large proportion of the workforce is qualified at PhD level. 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 to ensure they do not deter graduates from joining defence industry. This includes the length of time it can take to obtain, as well as requirements around maintaining a clearance. Industry consultations

have also shown 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. These companies are global and without the added complexities of citizenship or security clearance requirements. Left unaddressed, the inability to access specialised engineering knowledge will limit Australia's ability to expand a sovereign industrial capability in surveillance and intelligence in the digital sectors. 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 a security clearance, with 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 pulling in different directions—inhibits innovative ideas transitioning into service solutions. Defence recognises the value of collaboration in this sector and the Defence Innovation Hub will continue collaborating in the sector where possible. Defence also expects policy documents such as this Plan, which detail critical industrial priorities, to facilitate greater collaboration across industry and academia.

Global trade barriers

The sensitivity of advanced signal processing and surveillance and intelligence technologies typically limits the export market to a limited number of trusted partner nations. The United States is the biggest market, but also the most challenging to do business in, due to the complexities of its International Traffic in Arms Regulations (ITARs) and associated Export Administration Regulation requirements. Companies may need to consider the impact of ITARs on supply chains when seeking third party commercial opportunities. Australian industry must also compete with global businesses that enjoy greater economies of scale and access to cheaper labour and materials.

The trend towards networked sensor fusion—and greater integration of tactical sensors with ADF and Five Eyes C4I systems—is expected to constrain future participation in this Priority by Australian industry entities with foreign ownership or controlling interests.

The critical importance of Five Eyes interoperability is driving adoption of 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, which contribute 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 entities with non-Five Eyes foreign ownership or controlling interests. Without access to the necessary technical information, industry will be disadvantage in the Australian and wider Five Eyes defence industry marketplace, no matter how independently capable their technologies or solutions are. Australia needs to maintain its trusted relationship in the collaborative partner community, and ensure the Australian workforce is able to work on new technologies in this domain. This will be of benefit to Australia and our Five Eyes partners.

Security

Threat actors seek access to privileged information on Australia's military capabilities. Surveillance and intelligence 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'.

Government action

Establish a communications security industry engagement strategy

Defence will develop a strategy to establish an effective partnership that maximises opportunities for Australian industry to provide accredited Communications Security (COMSEC) support to Defence. The modalities for the partnership will be agreed, and an effective governance model for improved COMSEC industry engagement by Defence will be developed.

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 industry 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 delivery and enhance Australia's industrial base.

Industry capability enablers

Through broad consultation with Defence and defence industry, analysis of the value chains and consideration of the ADF's strategic ambitions and outlook, four driving enablers for the Surveillance and intelligence and Advanced signal processing priorities have been identified that must be accessed or controlled by Defence to protect our sovereign interests.

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.

1 AGILITY WITHIN THE SECTOR AND DEFENCE

Agility and flexibility are critical to ensure that ADF technologies, sensors and capabilities can keep pace with the rapid refresh rate of technologies in these industries, as well as the changing security landscape. To maintain the ADF's warfighting advantage, industry must be flexible enough to cater to software and software-defined hardware that may need to be updated weekly. This requires an agility focus from both Defence and industry to rapidly deliver software engineering solutions that meet the ADF's needs.

Agility within the defence industry sector will ensure the ADF has the advanced signal processing and surveillance and intelligence capabilities to meet its current and future needs. Key to this will be an awareness of upcoming Defence projects and capability needs.

2 SECURE COLLABORATION INFRASTRUCTURE

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

Traditionally there is significant expense and lead time required to accredit new facilities and networks. This considerable barrier to entry has resulted in only very established members of this industry having accredited infrastructure, and has limited growth of new businesses into the sector. Further, collaboration and information sharing between industry has 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 a limited number of trusted international partners.

Government action

Cyber readiness

The Australian Department of Defence will support industry to align their cyber security processes to meet new international frameworks, by providing grants to small to medium-sized businesses that have projects aligning to one or more of the Sovereign Industrial Capability Priorities through the Sovereign Industrial Capability Grants program, supporting them in gaining the required certification. This will ensure Australian industry can continue to export to the United States 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. This results in 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 real 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 for compliance with relevant standards to ensure interoperability-by-design.

A SKILLED AND CLEARED WORKFORCE

A highly educated and skilled workforce with the necessary levels of security clearance—and a good understanding of Defence missions and its needs—is a critical enabler of this sovereign industrial capability.

The level of training and experience required to develop leading-edge sensor and signal processing capabilities requires a 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 some other industries.

Mechanisms already exist for industry to obtain security clearances for their workforce, but obstacles can arise because of the time needed to complete clearance processes. Defence is exploring opportunities to offer more unclassified work packages to industry. This will help build business confidence to invest in recruiting and vetting their workforce.

Platforms and technologies that deliver advanced signal processing will continue to be replaced and upgraded. Workforce knowledge and understanding will be critical to ensuring a long-term digital capability in Australia. Essential talent in software development and engineering, information technology, data science and electronics, or other specialist engineering capabilities, are key enablers for this industry.

Government action

Skilled workforce development

To support workforce development in surveillance and intelligence 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.

Connecting Defence and the Australian Space Agency

The creation of the Australian Space Agency in 2018 has led to significant federal and state funding to build and strengthen a sovereign space industry. Grants and incentive programs, as well as substantial university involvement, are enhancing research and development and enabling small, entrepreneurial businesses to thrive. Adjacent industries outside of the space sector are also considering investment opportunities in space. The similarities between the space industry and surveillance and intelligence industries enables government to leverage space industry solutions to solve Defence-specific problems. Defence works together with the Australian Space Agency to identify future needs and support the development that could be leveraged from the civil space sector.

The Surveillance and intelligence Priority emphasises the significance of digital space technologies in generating ADF warfighting advantages, now and into the future. The space and cyberspace domains will become increasingly important for Defence capability and it is critical that Australian industry is developed to support the ADF. There is room for more defence-specific space businesses to grow in Australia, and Defence can use this as an opportunity to leverage the growing Australian space industry to support Defence capability.

It is not the intention for Defence to be a competitor to the commercial space sector, but rather to support organisations that are either already delivering to Defence and seeking to grow their space capability, or those that currently provide government and other customers a space capability that could be applied to a Defence context. Defence will need trusted partners in the space and other adjacent industries that can meet the additional security requirements needed to support the ADF and its allies.

Government action

Greater information on Australia's vision for space

In April 2019 the Australian Government released *Advancing Space: Australia's Civil Space Strategy 2019-2028* which outlines the Government's plan to transform and grow our space industry over 10 years, including tripling the Australian space sector and creating 20,000 new jobs.

Included in this strategy were seven National Civil Space Priority Areas, and the Agency will release roadmaps highlighting opportunities for investment in each of these priorities from the end of 2020. A coordinated effort between Defence and the Agency will ensure the capabilities are developed to support aspects highlighted in this Plan.

CASE STUDY

The Australian Space Agency

The purpose of the Australian Space Agency (the Agency) is to transform and grow a globally respected space industry to lift the broader economy, and inspire and improve the lives of Australians. As Australia's national civil space agency, it coordinates civil space matters across government and supports the growth of the Australian space sector.

Australia's geographic location and capabilities in transferrable technologies make it well-placed to capture value from the rapidly growing space sector. The Australian Government aims to triple the space sector market size to $12 billion and create up to an additional 20,000 jobs by 2030, with further jobs and economic growth from spill-over effects.

The Agency is responsible for delivering key space programs that develop national space capability and infrastructure, unlock international space collaboration, and inspire and build a future space workforce. It is also the regulator of Australian space related activities and a facilitator for collaboration across industry, government and academia.

The $150 million Moon to Mars initiative provides funding for Australian businesses and researchers, focused on creating jobs for Australians and strengthening Australian industry. It will support the transformation of industries across the economy and accelerate the growth of the space sector by providing opportunities to enter international supply chains, increasing demand for new capabilities, creating inspiration and enabling spin-out technologies for economic growth.

In addition, the $15 million International Space Investment initiative supports projects that grow the Australian space industry and build collaboration with international space agencies, and the $19.5 million Space Infrastructure Fund supports discrete facilities enabling the Australian civil space economy to develop. The Australian Space Agency is also establishing the Australian Space Discovery Centre to inspire the next generation to take up careers in science, technology, engineering and mathematics, and support the growth of the future workforce.

The Agency will release technical roadmaps for each of the National Civil Space Priority Areas outlined in Advancing Space: Australian Civil Space Strategy 2019-2028. These roadmaps underpin the Agency's vision for the sector and highlight investment opportunities, many of which will identify capabilities aligned with this Plan's outcomes. A coordinated effort between Defence and the Agency will ensure the capabilities are developed to support aspects highlighted in this Plan.

Further information can be found on the Agency website at www.space.gov.au.

ANNEX A. GOVERNMENT ACTIONS

This Plan includes the following actions to be taken by Government 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.

Theme	Government Action	Responsible	Timeframe
Establish a COMSEC industry engagement strategy	Defence will develop a strategy to establish an effective partnership that maximises opportunities for Australian industry to provide accredited COMSEC support to Defence. The modalities for the partnership will be agreed, and an effective governance model for improved management of COMSEC industry engagement by Defence will be developed.	Joint Capabilities Group	2021
Cyber readiness	Defence will support industry in aligning their cyber security processes to meet new international frameworks, by providing grants to eligible small to medium-sized businesses to support them in gaining the required certification. This will ensure Australian industry can continue to export to the United States and actively participate in global markets. Industry will be able to apply for these grants through the current Sovereign Industrial Capability Grants program.	Strategy, Policy, and Industry Group	Until 30 June 2022
Workforce development	To support workforce development in surveillance and intelligence 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
Space industry development	In April 2019 the Australian Government released *Advancing Space: Australia's Civil Space Strategy 2019-2028* which outlines the Government's plan to transform and grow our space industry over 10 years, including tripling the Australian space sector and creating 20,000 new jobs. Included in this strategy were seven National Civil Space Priority Areas, and the Agency will release roadmaps highlighting opportunities for investment in each of these priorities from the end of 2020. A coordinated effort between Defence and the Agency will ensure the capabilities are developed to support aspects highlighted in this Plan.	Australian Space Agency with support from Defence	Ongoing

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 sector. This system will support companies that contribute to the generation of this Priority to innovate further, and position them 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 2030 More, Together: Defence Science and Technology Strategy for innovation and clear resourcing plans. These programs have also been bolstered by various measures of the Government's economic stimulus package; aimed at supporting the COVID-19 economic recovery 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 for business 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 $2,500 to $150,000 for small-to-medium enterprises to fund part of the cost to engage a consultant or expert to implement recommendations. Capability Improvement Grants reimburse a business for up to half the cost of engaging a consultant or expert to assist with skills and training, to 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 $15,000 to $150,000 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 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 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 Priority grants are capped at $3 million over three years and are delivered through the Centre for Defence Industry Capability. These grants directly subsidise the growth of industry in the industrial capabilities underpinning the Priorities and are for more mature companies that are able to fund at least 50 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 (mentees) 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