

**Submission to:**

**Inquiry into the performance of  
the Department of Defence in  
supporting the capability and  
capacity of Australia's defence  
industry.**

14 July 2023

**Sovereign Australian Prime Alliance**



## About SAPA

The Sovereign Australian Prime Alliance (SAPA) is an informal grouping of large Australian prime contractors to the Federal Government. We comprise:

[AUSTAL](#) - Australia's global shipbuilder;

[Gilmour Space](#) - Australia's leading venture-capital-backed space technology company;

[Macquarie Technology Group](#) - Australia's data centre, cloud, cyber security and telecom company; and

[NIOA](#) - Australia's leading weapon system and integrated soldier systems provider and supporter.

SAPA formed in 2022 to advocate the important economic and social contributions sovereign Australian prime contractors provide the Australian economy - including to Australian SMEs - and to push for genuine sovereign capability in areas that are critical to Australia's national security and defence interests.

Our shared goal is to advocate for Federal Government to cultivate and support Australia's sovereign prime contractor companies in the interests of achieving a more self-reliant Australia, and supporting policies the current Government took into the 2022 Federal Election. Specifically:

- Future Made in Australia (FMIA); and
- Buy Australian First Plan

### 1 INTRODUCTION

- 1.1 SAPA welcomes this opportunity to contribute to the Foreign Affairs, Defence and Trade Committee (the Committee) *Inquiry into the performance of the Department of Defence in supporting the capability and capacity of Australia's defence industry* (the Inquiry).
- 1.2 In aggregate, SAPA represents significant human resources (ie. combined workforce nearing 2,000), financial capital (ie. combined valuation in excess of \$3 billion), and technical capability (eg. registered patents).
- 1.3 Our people work in the service of Australia's national security and defence, and our investments are overwhelmingly focused on Australia, whether they be advanced manufacturing facilities in Queensland, shipyards in Perth, or data centres in Sydney and Canberra.
- 1.4 Our significant investments in research and development are applied almost exclusively here in Australia, and we provide capabilities that are all currently listed by Defence as Sovereign Industrial Capability Priorities (SICPs).

## 2 FIRST PRINCIPLES

- 2.1 **Definition of 'sovereign supplier':** SAPA defines a "sovereign supplier" as an Australian company that is not a foreign subsidiary, that is based in Australia, controlled by Australian shareholders, and governed by an Australian Board of Directors.
- 2.2 **Definition of Australian prime contractor:** SAPA defines an Australian prime contractor as an Australian company that is not a foreign subsidiary, that is based in Australia, controlled by Australian shareholders, and governed by an Australian Board of Directors.
- 2.3 **Definition of 'Australia':** Where the Terms of Reference refer to Australia's (or Australian) defence industry capability (or simply Australia's defence industry) we assume this to mean Australian companies that are not foreign subsidiaries, that are based in Australia, controlled by Australian shareholders, and governed by an Australian Board of Directors.

## 3 RECOMMENDATIONS

- 3.1 **Recommendation #1:** *Defence Industry Development Strategy (DIDS) adopt the SAPA definition of 'sovereign', as described in paragraph 2.1.*
- 3.2 We are aware of a current debate within the Department of Defence ('Defence') as to how the DIDS will define 'sovereign capability'. It is critical Defence's definition of sovereign in the context of industrial capability align with the definition of sovereign as used in the context of 'sovereign risk'.
- 3.3 Australia's sovereign risk cannot be assessed against the quantum of Australian denominated currency everywhere in the world. Likewise, our industrial capability should not be assessed against the quantum of companies - Australian and foreign - which provide capability to Defence.
- 3.4 Just as it is beyond the control of the Commonwealth to seize every Australian dollar in the world to support its' sovereign risk, it is likewise beyond its' control to seize the full international capability applied to support Australia's defence and national security.
- 3.5 **Recommendation #2:** *The DIDS to define international and domestic capabilities as separate, complementary lines of industrial activity - ie. Domestic Capability and International Capability, with domestic capability being defined as "an Australian company that is not a foreign subsidiary, that is based in Australia, controlled by Australian shareholders, and governed by an Australian Board of Directors".*
- 3.6 We understand there is view among some within Defence that 'built in Australia' should be the acceptable threshold for being defined as sovereign (to Australia). If this were to be written into the DIDS it would generate multiple negative outcomes for Australia.
- 3.7 Primarily, it will create an illusion of jurisdictional control over international capability providers. Regardless of contractual pledges of foreign owned entities, the jurisdiction of Australian Courts does not extend outside our shores and would require cooperation from other international jurisdictions (for service of proceedings or injunctions to prevent the commencement of action against Defence in foreign Courts) or the cooperation of the foreign owned corporate itself. This can never be guaranteed even in peacetime, much less during times of conflict, and would create unnecessary risk to the Commonwealth if applied.
- 3.8 SAPA acknowledges the important contribution international defence primes make to Australia's Defence capability and our national security. However, we do not see any legitimate argument for naming international corporations as sovereign to Australia.

- 4.1 Identifying capabilities as two separate streams - domestic and international - would have no detrimental impact to the international primes supplying the Australian Defence Force (ADF), but would have an immediate positive impact on Defence's application of current government policy (ie. Buy Australian First and FMIA) and would also help bolster Australia's national security since it will enable focused strategy by Government on the development of genuine sovereign capability in specific, critical capability areas.
- 4.2 It would also assist with future policy development where Defence and Government might seek to direct Government effort towards specific capability areas where Australia has critical mass, critical need, or other imperative.
- 4.3 **Recommendation #3:** *Defence must ensure any revisions to the SICPs not exclude any of the following capabilities from the SICPs list:*
- *continuous shipbuilding;*
  - *guided munitions and explosive ordnance;*
  - *space; and*
  - *cyber security.*
- 4.4 The case for the permanent inclusion of the above capability areas as SICP is articulated concisely and compellingly in the Defence Strategic Review (public version).
- 4.5 The DSR case for the permanent inclusion of **Cyber as a SICP**: The DSR is unambiguous in calling out cyber as a military domain in its own right:
- *"The current joint force, namely the combined effect of Navy, Army and Air Force working together, does not appropriately reflect the growth of domains. The evolution to five domains - maritime, land, air, space and cyber - demands a new approach."*
- 4.6 The DSR is also unambiguous in articulating the need for Defence to scale up its cyber capability:
- *"Australia's cyber and information operations capabilities must be scaled up and optimised."*
  - *"Defence must enhance its cyber domain capabilities to deliver the required responsiveness and breadth of capability to support ADF operations."*
- 4.7 Given this unambiguous advice to Defence that Australia needs to scale up its cyber defence capability, it would be illogical for cyber not be listed as a SICP. This advice is supported by leading voices in the civilian cyber sector.
- 4.8 Of relevance is annual research published by AustCyber examining the human resource capacity Australia needs to meet the growing cyber threat. According to the AustCyber Annual Competitiveness Report 2022, there will be 3,000 fewer cyber security workers than required in Australia by 2026.<sup>1</sup>
- 4.9 Unlike some of the more nascent critical technology capabilities Defence is pursuing, Australia's cyber security sector is already operating at scale<sup>2</sup> and has scope to expand further in partnership with Defence.
- 4.10 Furthermore, the case for Defence to support Australia's sovereign cyber security sector is supported by recent research and policy declarations, specifically noting national security interests inherent in cloud and data storage/ processing capabilities which remain onshore

<https://www.austcyber.com/resources/sector-competitiveness-plan>

Ibid, Australia's cyber security sector contributes \$4.2 billion annually to national GDP and is supported by over 47,000 workers.



under the protection of security-cleared Australian citizens, and under the jurisdiction of the Australian Government.

- 4.11 Dr Rajiv Shah, in the Australian Strategic Policy Institute's Report No. 56/2021 underscores the role of sovereign capability in cybersecurity. He notes:

*"The importance of sovereign capability is broadly accepted as a general concept, and a prioritisation framework for sovereign capability should be developed and actively managed in order to direct further policy interventions. Buyers of cybersecurity products and services should be encouraged to understand the opportunities that come with support for growing local companies, starting with better leverage of government procurement; this should include a 'Buy Australian' mandate linked to sovereign capability priorities."*<sup>3</sup>

- 4.12 This was recognised in Prime Minister Albanese's speech to the Lowy Institute in March 2022 in which he noted:

*[S]overeign, domestic data security is a modern foundation of national security...[and] the storage of our data--much of which is offshore--has implications for our sovereignty and security. For some types of data, appropriately securing it may require mandating that it be kept in Australia."*<sup>4</sup>

- 4.13 As noted earlier, there exists sufficient capability and capacity within Australia's sovereign cyber security sector to deliver the cloud and data storage/ protection services required by Defence and, if necessary, sufficient capital to scale up further.

- 4.14 Many of Australia's sovereign cyber security companies are already providing their services to civilian government agencies but have struggled to get traction with Defence despite the political and policy views from the notable sources quoted in this submission, notwithstanding input from other credentialed sources<sup>5</sup>.

- 4.15 The DSR case for the permanent inclusion of **Guided Weapons and Explosive Ordnance as a SICP**: The 2023 Defence Strategic Review, the 2020 Defence Strategic Update and 2020 Force Structure Plan outlined the need for the Australian Defence Force (ADF) to act with greater independence in an increasingly contested strategic environment, and highlighted that the establishment of a Guided Weapons and Explosive Ordnance Enterprise, development of a more durable supply chain is critical to the ADF's self-reliance.

- 4.16 On 31 March 2021, the then Government announced the acceleration of a Sovereign Guided Weapons and Explosive Ordnance (GWEO) Enterprise to enhance Australia's self-reliance and supply chain resilience.

- 4.17 Under the 2020 Force Structure Plan, the ADF is expected to acquire somewhere between \$74 billion and \$110.7 billion (2020 dollars) in Guided Weapons. Accordingly, it makes both military and economic sense to manage these programs holistically in order to achieve permanent sovereign industrial outcomes.

- 4.18 Australia does not currently own the intellectual property to manufacture our own complete guided weapon systems. We are heavily dependent on international companies to supply guided weapons who hold the IP to manufacture these weapon systems. Our ability as a nation to defend ourselves is therefore heavily reliant on the continuity of overseas supply which may be constrained or blocked in time of conflict.

<sup>3</sup> Australia's Cyber Security and National Security; Dr. Rajiv Shah, Australian Strategic Policy Institute's Report No. 56/2021

<sup>4</sup> Anthony Albanese, *Stronger in the World, United at Home*, (Speech to the Lowy Institute, Canberra, 10 March 2022).

<sup>5</sup> For further reading see Andrew D Mitchell, *Sovereign Cloud Services: Data localisation requirements & Domestic Government Procurement Preferences* (Monash Law, 24 May 2021) [290].

- 4.19 The DSR case for the permanent inclusion of **Naval Shipbuilding as a SICP**: The DSR highlighted the importance of a national shipbuilding capability by calling for a continuous shipbuilding capability.
- 4.20 In 2018 continuous shipbuilding was designated as a SICP. But, despite 8 of the 10 SICPs having mature delivery plans, none was developed to deliver Australia a continuous shipbuilding objective. The result has been a lack of long-term shipbuilding planning, manifested in part through a lack of consolidation on the Henderson Precinct in Perth. This has had detrimental long-term impacts on shipbuilding with recurrent valleys of death still evident in Western Australia. This lack of certainty and stability has had a detrimental impact on the local workforce, and in turn on Australia's national security since much of the intellectual capacity to build ships has been lost due to the absence of proper strategic planning.
- 4.21 The solution is to have continuous shipbuilding nominated as a SICP. This will ensure a comprehensive plan is developed and measured that supports selected shipbuilders to build essential platforms for the ADF, free of the reliance on other international shipbuilders, focused on output that suits their commercial priorities, not Australia's.
- 4.22 One of the objectives of the SICPs should be to require technology transfer by international primes designing and building vessels in Australia. This requires Government and Defence oversight and should be part the Value For Money (VFM) decision when selecting a Prime, in the absence of a local capability.
- 4.23 Over time this will develop companies such as ASC such that future shipbuilding will be possible led a sovereign Australian company, where this current capability is deemed not to exist. The same logic should apply in Western Australia, although there is already the capability for patrol vessel and specialist ship building resident in Australia.
- 4.24 In the current uncertain geopolitical environment, there is a need for a greater sense of urgency to achieve supply chain resilience as a matter of priority. The COVID pandemic has proven this need. Continuous shipbuilding is a national security issue, and it needs focus by Government and delivery by Defence to recognize it as a SICP and put this into full effect.
- 4.25 The traditional method of ship procurement takes too long from Tender to cut steel and invites unnecessary competition and inefficiencies. The result can be multiple, diverse and less resilient supply chains and increased risk associated with builder start-ups.
- 4.26 However, this elongated competitive process is in accordance with current Commonwealth Procurement Rules (CPRs). Notwithstanding, the authors of the CPR did foresee there would be occasions when the CPRs need not apply. One of these is when essential security interests are at stake<sup>6</sup>. This would apply to the current security environment where for example, global uncertainty and volatility is increasing and strategic warning time for conflict has been substantially reduced.
- 4.27 A continuous shipbuilding SICP is required to ensure the national shipbuilding industry is lock step with and operating in support of our national security. To outsource shipbuilding offshore in the current environment is a high-risk decision that makes the ADF and Australia more vulnerable than it need be.
- 4.28 There is one current example for shipbuilding to follow - the active phased array Radar SICP delivered by CEA Technologies (CEA), a sovereign Australian prime. Through a committed approach to developing a priority sovereign capability, supported by Government funding and partnership, CEA has grown into a world class capability that is truly sovereign, with sovereign IP resident in Australia.

- 4.29 To that end, CEA supports local supply chain resilience and innovation rather than having to rely on foreign supply chains. The intellectual property remains in Australia, as does continuous research and development. Continuous shipbuilding requires the same level of focus, development and certainty over time, particularly in this period of regional and global uncertainty.
- 4.30 The DSR case for the permanent inclusion of **Space as a SICP**: As with cyber, the DSR is also unambiguous in defining Space as a military domain.
- 4.31 Currently the Australian Government has no sovereign capability to access and operate in the space domain. Paragraph 4.12 of the DSR defines resilience as “the ability to withstand, endure and recover from disruption”, and notes that “Resilience makes Australia a harder target and less susceptible to coercion”, before going on to establish “robust space capabilities” as a critical requirement for national resilience.
- 4.32 The need for sovereign capabilities to access and operate in space through domestic launch facilities, an associated responsive launch capability, and satellite development and integration, are critical to ensure Australia will have the ability to withstand, endure and recover from possible space domain disruption. Such sovereign capability will directly contribute to the deterrence called for in paragraph 4.13 of the DSR.
- 4.33 Both paragraph 8.49 and 8.50 acknowledge the relevance of both civil and commercial space capabilities to Defence’s own space capabilities, identifying the importance of commercial capabilities in “complementing and augmenting Defence’s Space Command structure”.
- 4.34 For the DSR’s space domain recommendations to be achievable and sustainable in the medium to long term, a vibrant and thriving sovereign space industrial base is essential. Whilst a sovereign commercial space industrial base is not reliant on Defence, for Defence to be reliant on it, Defence must list space as a SICP.

-END-