AUKUS Pillar 2 critical pathways

A road map to enabling international collaboration

GEORGE HENNEKE
ROLAND STEPHENS

MAY 2024

Special Report

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

About the authors

George Henneke is a former senior defence economist at ASPI. He has previously worked for the US Government and has experience working in defence and space industry.

Roland Stephens leads the client function for a government backed asset manager and central borrowing authority. Before that he established and led Austrade's defence team and spent over a decade as a natural resources investment banker.

Acknowledgements

The authors thank the many contributors and colleagues who offered their time and insight to this research project, including all peer reviewers and ASPI staff who worked on this project, especially Bec Shrimpton. Companies including Raytheon Australia, Leidos, SYPAQ, Hypersonix and Mellori Solutions offered their time and insights with enthusiasm. William Greenwalt and James Tennant offered their deep experience in the fields of defence industrial policy and finance. We thank the more than 170 organisations that participated in the project, including by providing valuable insights, with specific depth from Adarga, Advanced Navigation, APC Technology Group, Asension, BAE Systems, Blacktree Technology, Brassets Group, C2 Robotics, Defence Industry Advisory Services, DINGO, DroneShield, Hensoldt, Inovor Technologies, J3Seven, L3Harris, Lawforce Alpha, Maxwell Capital, Noetic Group, Nova Systems, Ocius, the Office of Defence Industry Support, Prism Defence, QuintessenceLabs, SAHR Professional Services, Skylark Labs, Southwest Research Institute and Thales Australia.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

About Special Reports

Special Reports are written by both internal and external authors, they are intended to deepen understanding on critical questions facing key strategic decision-makers and, where appropriate, provide policy recommendations.

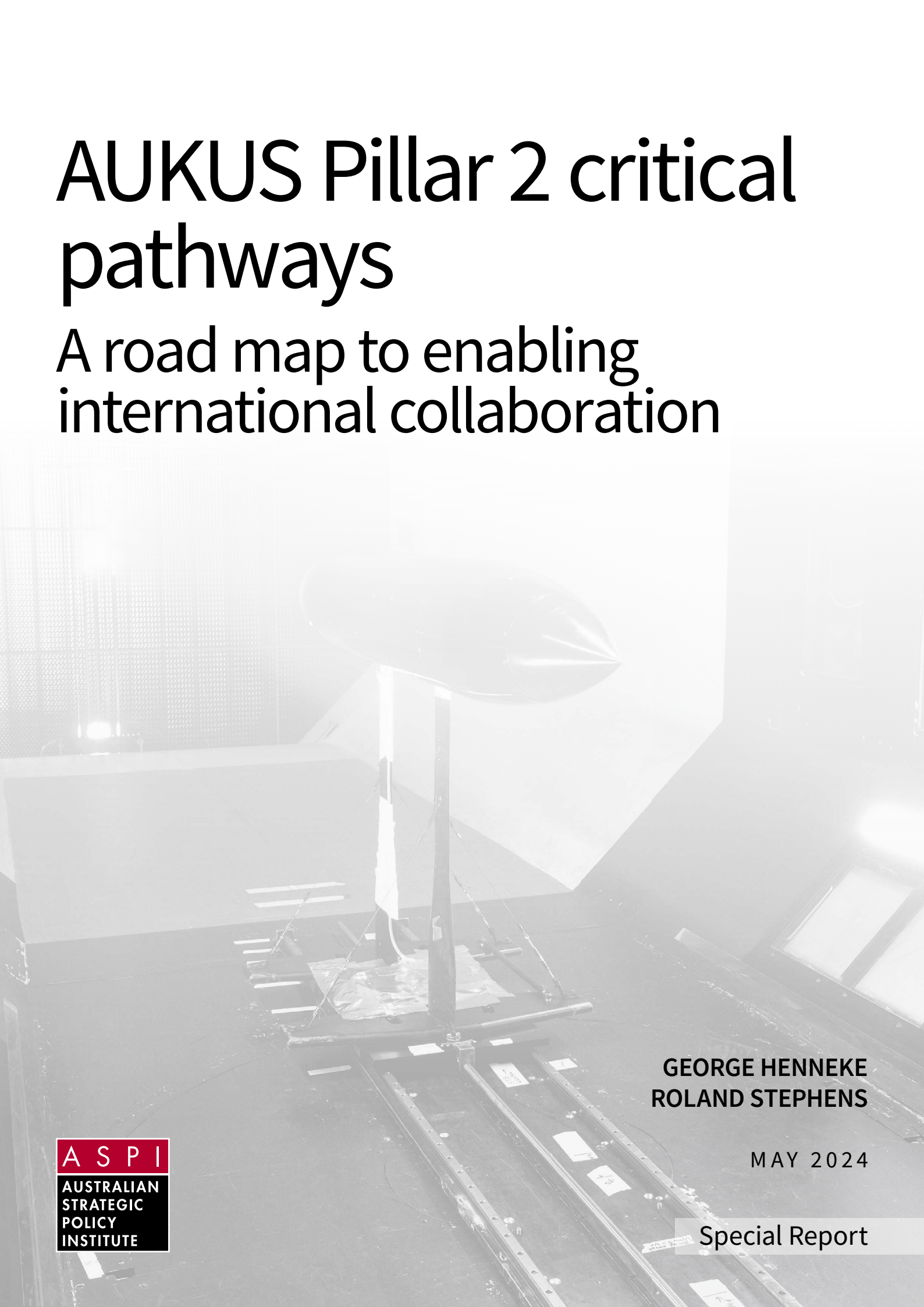
Funding

Partial funding for this report was provided by Raytheon Australia and Leidos.

Cover image: Defence Science and Technology wind tunnel, Melbourne, Victoria, Defence image library, online.

AUKUS Pillar 2 critical pathways

A road map to enabling international collaboration



GEORGE HENNEKE
ROLAND STEPHENS

MAY 2024

Special Report

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

First published May 2024

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Tel Washington DC +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

 Facebook.com/ASPI.org

 @ASPI_org

Contents

Executive summary

The AUKUS trilateral partnership presents Australia with an unprecedented opportunity to achieve national-security goals that have eluded it for decades. It could offer access to cutting-edge technologies. It can further integrate Australian, US and UK military forces, allowing more unified action to maintain deterrence against national and transnational actors who threaten the global rules-based order. Perhaps most importantly, AUKUS—in particular its Pillar 2 objectives—is an opportunity for Australia to pursue the long-sought industrial capacity necessary to defend its borders and its interests across a range of probable conflict scenarios.

A vision for Pillar 2 success

AUKUS partner nations implement operational and regulatory frameworks to co-produce, co-field and continuously enhance world-leading national defence capabilities in critical technology areas. Governments will provide leadership and resources to drive effective multinational collaboration among government, industry and academic contributors, leveraging competitive advantages from across the alliance to deliver collective capability.

Whatever the rhetoric, however, the benefits are far from assured. While the effort has had successes, including cooperative artificial intelligence (AI) / autonomy trials and landmark legislation,[1] most of the hard work remains. Strategies and principles are only the beginning. Success or failure will hinge on the translation of those strategies and principles into the regulations, standards and organisational realignments necessary to operationalise the vision. The challenges are significant—from skills and supply to budgets, leadership and bipartisanship. But the benefits from this three-nation enterprise are worth the hard work to sustain political will and financial investment and to combine aspirational ambition with suitable risk tolerance to overcome obstacles.

Past debate has contributed valuable insight into problems that can threaten the full realisation of the AUKUS arrangement including for example, problems like outdated and dysfunctional export-control regulations, struggles with integrating complicated classified information systems and differing regulations and frameworks among the AUKUS partners. Yet, when it comes to fixing those problems, regulators and industry participants often talk past one another. Governments claim that mechanisms are in place to facilitate cooperation.[2] Businesses counter that waiting six months or more for necessary approvals is an unreasonable impediment to innovation.[3] Both sides have a point. So far, reform efforts have been unable to break the logjam.

In this study, ASPI takes a different approach. Rather than wade once more into the morass of trade regulations to identify obstacles and recommend fixes, we interviewed the regulators and businesses that implement and operate under those regulations. Our data collection involved engaging more than 170 organisations as well as key individuals. Our intent here is to provide an operational perspective on practical barriers to cooperation as envisaged under AUKUS—particularly under Pillar 2—and offer the Australian Government detailed and actionable recommendations that we believe would help AUKUS Pillar 2 succeed.

A constant challenge has been policymakers' lack of understanding of the daily challenges faced by businesses striving to keep Australia, the US and the UK at the forefront of defence innovation.[4] Similarly, myths abound among industry participants about the degree of restrictions imposed by regulations such as the US's International Traffic in Arms Regulations (ITAR).[5] Officials make the claim that all necessary exemptions exist for AUKUS partners to cooperate,[6] and that only minor adjustments are required to turbocharge transnational innovation. Businesses reply that narrowly tailored exemptions buried in mountains of rules are useful only for the lawyers required to make sense of them. This report aims to bridge that gap.

AUKUS is a generational opportunity for Australia. Its focus on critical Pillar 2 technologies has the potential to bring Australian champions to the world stage and lift the nation's defence industry up to the state of the art in a range of modern capabilities. Done right, that can help to realise the robust industrial capacity that Australia needs.

The R&D gap

Regulatory reform is critical to Australia's success under AUKUS Pillar 2. But, regardless of any resulting improvements, the nation's defence industry will struggle to compete with international partners at current levels of public R&D funding.

Allocations to the Defence Science and Technology Group in the 2023–24 Portfolio Budget Statements amounted to less than 5% of Defence's capability acquisition program.

In contrast, appropriations by the US Department of Defense to early-stage R&D activities were nearly 40% the size of its procurement budget in its FY 2024 budget request. The full US research, development, testing and evaluation budget of over US$145 billion goes not only towards advanced technology but to the defence industry's capacity for operationalising the resulting capabilities.

Tax incentives can help, but they aren't a replacement for direct investment. Public funding feeds industry's technology development pipelines, filling critical gaps in early-stage research where businesses struggle to profit from direct investment.

Intellectual property (IP) developed through public-sector R&D is an important part of US defence acquisition strategies. For example, the open-systems approach seeks to accelerate system upgrade timelines and encourage competition by maintaining government control of core technologies, but turning to industry for plug-and-play components.

Government-funded IP development is an important enabler for private businesses. Contracted research, development and engineering activities build corporate knowledge, regardless of who owns the resulting IP. Businesses build relationships with government laboratories, innovators and requirements developers, strengthening the collaborative networks critical to successful defence innovation.

But the driving force of private industry is profit. Businesses are not and should not be charitable organisations. Contractual arrangements must leave opportunities for them to invest their own money in key technologies, thereby establishing IP ownership for critical components and ensuring long-run profitability. Acquisition officials must carefully weigh such considerations if they wish to build a competitive defence industry that can succeed in an AUKUS context.

Public funding of early-stage R&D is probably the single biggest factor that's made the US defence industry what it is today. Coupled with the bleeding-edge capability being developed in the commercial sector, it's the most glaring gap in Australia's defence industrial strategy. The less Australia supports its domestic industry through comparable provision of publicly funded R&D—and the less it can articulate a sound IP strategy that rewards private investment while securing long-term government interests—the more vital it becomes to facilitate Pillar 2 channels through which Australian businesses can participate in US or UK programs.

Recommendations for the Australian Government

Australian industry—and the government supporting it—will face a steep learning curve throughout the radical regulatory reform necessary to realise the objectives of AUKUS Pillar 2.

The Defence Industry Development Strategy (DIDS), released on 29 February 2024, picks up some of the issues that we raise in this report.[7] It recognises, for example, a need for joint structures and investments with partners, such as genuine multinational cooperative research centres, which can help build the Australian defence innovation ecosystem. This report offers key recommendations that, if implemented, offer a pathway to execute elements of that strategy. The DIDS can't be viewed in isolation from proposed defence export-reform legislation. The strategy itself makes the link between Australian defence business success and access to export markets.

It's vital to acknowledge up front that most of the businesses that will be the foundation of Australian industrial growth have neither the knowledge nor the resources necessary to achieve and maintain compliance with many of the proposed reforms. Indeed, ASPI's research strongly suggests that such knowledge and resources don't exist in sufficient quantities within the Australian economy. The government must therefore play an outsized role in jump-starting growth. Its effort

should address 12 key recommendations identified in our research.

The Australian Government should do the following:

1. *Empower and resource Defence Export Controls (DEC), the Defence Industry Security Program (DISP) and similar organisations as critical agents of Australian competitive advantage.* Ask anyone about the central problem of defence-industry cooperation between Australia and the US and the first thing they'll mention is the US's ITAR. AUKUS is an opportunity for Australia to empower its domestic industry and thus the entire alliance by doing regulation better. It must invest in a public-sector workforce with both commercial and security backgrounds, including deep expertise in the technological and legal aspects of the defence industry and the adjacent dual-use space. It must streamline processes for the transfer of technical data to enable joint development and production. It must align export-control regulation of defence goods and services with best practices of partner nations, while learning from their mistakes. And it must do everything faster.

2. *Consider both public- and private-sector organisational incentives.* Avoiding past mistakes means doing things differently.[8] Arguably, the single biggest problem with existing systems—from ITAR to DISP—is poor risk management. Leaders articulate a new vision, while those at the working level are rewarded for maintaining the *status quo* and disincentivised to take risks. Legislation being initiated across partner countries sets us off on that same path, establishing appropriate authorities but leaving the details up to organisations that have perpetuated dysfunctional execution. Organisational reform must accompany regulatory reform, incentivising frontline administrators to appropriately balance security with joint industrial development outcomes. There must be a focus on the incentives for business to engage with the AUKUS endeavour. That includes solving questions relating to IP ownership through contract mechanisms governing funded research. Businesses must establish the relevant experience and relationships through collaborative R&D—with each other and with Defence—that spurs a virtuous and competitive growth cycle.

3. *Establish expert-led governing bodies for AUKUS to manage ambiguity and surprise.* The path to success in AUKUS Pillar 2 won't be easy, and governments must expect the unexpected. There are many unknowns that will be discovered only through trial and error. We must acknowledge that reality from the start and take active measures to manage surprises. That means the early establishment of governing bodies with requisite expertise (including in industry and the regulatory systems of other governments), visibility into ongoing changes and broad interagency authority to help adjust course.

4. *Implement a differentiated approach to regulating dual-use goods and technologies.* Dual-use goods and services require different treatment from sensitive military technologies. Australia's defence export-control rules, and proposed amendments to them, make insufficient allowance for fundamental differences between military and dual-use technologies. Efforts to align defence trade controls with ITAR are at the centre of current Australian export-control regulation reforms. Those efforts risk failing to learn from the US experience. The US has spent years creating two different regulatory regimes for managing defence and dual-use technologies, whereby dual-use technologies are managed not under ITAR but under the US's alternative Export Administration Regulations. Few in the US would claim that its system works perfectly, and technologies do get trapped in the 'grey zone' between the two regimes, but the lesson from making the distinction is important. Australia should devise a new way to properly assign technologies between two regimes—one focused on a narrow set of high-risk, militarily sensitive defence technologies and one enabling agility and speed in the management of technology transfer for dual-use goods. Australia needs to sharpen the regulatory distinction and better balance the need for information security against that of attracting broader defence-sector participation and investment. This will be essential for Australian industry and regulatory competitiveness.

5. *Support industry as it builds skill sets that are currently lacking in the Australian economy.* Many of the obstacles identified in this report—export-control regulatory compliance, industrial security, cross-border technical certification—require not just new rules,

but the people to implement them. Those people will require sophisticated skill sets that have historically seen far lower levels of demand than will be required in the future under AUKUS.

6. *Understand and account for the changing costs and benefits associated with industry supply-chain strategies.* Developing and refining an effective system of international trade in defence goods requires accounting for the complicated supply-chain relationships that provide competitive advantage to Australian businesses. Regulators must maintain closer relationships with those businesses to understand how changes affect costs and benefits and thus the viability of existing business models. Defence must carefully consider the investment case and business implications, especially for small and medium-sized enterprises (SMEs), when designing regulation, regulatory bodies, industry support programs and procurement processes.

7. *Don't focus on past winners or declare success over easy wins.* In this research project, industry participants across the spectrum of size, capability and technological focus areas voiced concerns that Australia's Department of Defence isn't listening to them. At the same time, Defence engages industry through organising industry events, soliciting feedback and attending and speaking at relevant conferences. Both government and industry have valid issues. So why the disconnect? Our research suggests that Defence is turning to those it knows best and has dealt with in the past—those with available time and resources to listen and respond in language that Defence can readily understand—but that group constitutes a biased sample. Success will demand substantial expansion of current outreach programs, and a shift to sharing problems and seeking solutions with fast-moving smaller technology companies, in addition to the defence primes with which strong and comfortable relationships already exist. Some of the smaller and newer defence industry players (or those Defence seeks to attract to the sector) can also create solutions funded by private capital, opening new opportunities for delivering defence capability. Success will require the government to send stronger and more consistent buying signals to a greater range of actors and actively seek feedback rather than just receiving it, especially from organisations new to and even beyond the defence sector. The effort must continue throughout the long transition period ahead.

8. *Recognise that synchronised and simplified regulations are the key to success.* Control of sensitive technologies is important. Achieving the state of the art in the most important defence systems demands that Australia also achieve the state of the art in protecting AUKUS technology secrets. Reaching that standard—and doing it efficiently and effectively—will foster trust and open the floodgates of international investment.

9. *Align Australian industrial security standards and data-sharing protocols better with the US system.* Most of the talk around AUKUS reform and collaboration focuses on export-control rules, but as important as protecting secrets is opening pathways to sharing them among those who need to know. Urgent investment is needed in collaborative associated infrastructure, information technology and cybersecurity. Australia's DISP must align better with the US's National Industrial Security Program (NISP), sharing resources, benchmarking and possibly even merging some critical functions. This isn't to suggest that the US NISP is the standard; AUKUS represents a genuine opportunity to reimagine and re-engineer a truly integrated and collaborative system that works for all actors. Defence must subsidise joint facilities where businesses can work and collaborate in a classified environment. Australia shouldn't wholly adopt the US system (nor should the UK). This once-in-a-generation opportunity should be seized to catalyse complementary reforms in the US system, lifting the combined enterprise to a new level of functionality and symbiosis that can genuinely support critical technology collaboration among the AUKUS nations and develop military capabilities at the speed and scale necessary to compete and win.

10. *Ensure compatible technology standards with AUKUS partners to lower barriers to collaboration.* The AUKUS nations' technology and certification standards are often incompatible and too inflexible to accommodate differences. Allied electromagnetic systems can interfere with one another if frequency bands are not carefully deconflicted. Technicians from the two nations face different requirements in manufacturing and handling energetic materials. Everything from

matching nuts with bolts to airworthiness certification requires common sets of standards through which industry partners can combine complementary capabilities. Success demands working together to address and fix those differences.

11. *Prepare Australian industry to win in a new acquisition environment.* The US defence industry may be large and successful, but it's also complicated and opaque. Challenges Australian businesses face in dealing with their own defence acquisition processes are unlikely to be reduced in such unfamiliar and competitive terrain. The Australian Government must dramatically expand its liaison programs, implement tools and training to facilitate business opportunities, and push for broader Australian access to US small-business preferential contracting and grant programs.

12. *Support scaling up, which requires access to capital from both public and private sources.* Businesses accustomed to serving niche products to a A$50-billion-a-year customer (Australia) will struggle to serve a A$1.3-trillion-a-year customer (the US). The Australian defence industry must possess not only the means to win US and UK contracts, but the resources to deliver at scale. That will take capital. Australia must create a range of financing options to support such efforts, including direct loans, private-capital incentives, and public–private partnerships.

Operationalising the AUKUS Pillar 2 vision

A common criticism of the AUKUS Pillar 2 vision is its lack of an organising construct: many of the businesses on which its success depends see the effort as grand strategy without operational execution. Successful collaborative R&D needs clear requirements, funding and a unified program-management construct.

Operationalising the Pillar 2 vision will require working through the wide range of obstacles identified in this report. As in any such large endeavour, that means learning by doing. Past efforts at integrating allied industrial bases failed because their driving force was top-down rather than bottom-up. They originated not with war-fighters and innovators, but with regulators in their Canberra, Washington and London offices.

AUKUS Pillar 2 will succeed only if it can flip that script. Throughout ASPI's conversations with defence-industry participants, we received many suggestions on how that might be accomplished. There's near-universal agreement that the initiation of collaborative technology development efforts must begin immediately, rather than waiting for regulatory reforms to point the way.

Each Pillar 2 technology priority (see box) should start with a test case with clear, narrowly defined objectives. Associated program offices should be jointly staffed and funded, with strong governance structures empowered to address the operational and regulatory hurdles that are certain to emerge. They could be patterned on existing R&D organisations operating in partner countries: perhaps Australian cooperative research centres or US federally funded research and development centres.

AUKUS Pillar 2 technologies

1. Advanced cyber
2. Artificial intelligence (AI) and autonomy
3. Electronic warfare
4. Hypersonics and counter-hypersonics
5. Quantum technologies
6. Undersea capabilities

Industry-led initiatives point the way. One example is a company called Adarga, which uses AI tools to enhance research, analysis and decision-making. The company is organising a demonstration that uses UK-owned processing tools to gather insights from a trilateral dataset and present findings to a US customer. Adarga's strategy of crawl–walk–run is widely replicable. It will start with unclassified, non-ITAR-controlled data to demonstrate initial operating capability. With a proven operating construct, participants can then incorporate more restrictive elements and work through the resulting challenges. Findings could be fed through governing mechanisms to inform ongoing regulatory reforms.

Given disparities in historical funding levels between the AUKUS partner nations, joint R&D efforts risk becoming vestigial appendages to well-developed US programs. Australia should thus be the lead advocate and organising force. The effort must incorporate nascent AUKUS Pillar 2 structures: agreeing on requirements through the International Joint Requirements Oversight Council, drawing expertise from the AUKUS Advanced Capabilities Industry Forum, and exploring public–private funding opportunities through the AUKUS Defence Investors Network.

Research methods and objectives

Much ink has been spilled in outlining problems with existing rules and cooperative frameworks on which the success of AUKUS Pillar 2 will largely depend. Policy recommendations have laid out in detail the reasons for past failures and the mechanisms necessary to ensure future success.[9] Yet solutions remain elusive.

ASPI takes a different approach in this examination of the problem. Rather than starting with existing policy and enumerating its deficiencies, our analysis begins with industry. We interviewed Australian defence-sector participants operating across the spectrum of AUKUS Pillar 2 technology priorities. They included SMEs, Australia's largest prime contractors, and offices within the Australian Department of Defence and government that interact daily with all of them. We sought the perspectives of the people who regularly navigate the system.

Our outreach and data collection covered more than 170 such organisations. Through written surveys, direct conversations and participation in industry expositions and government workshops, we collected feedback, identified critical themes and narrowed our focus to a select group of businesses that illuminate those themes. Through in-depth discussions with people ranging from chief executive officers to developmental engineers, we built case studies illustrating the obstacles faced by innovative companies stymied in their efforts to collaborate with international partners in developing the next generation of defence technologies.

Our three research objectives were:

1. *Understand how businesses navigate the system today.* We examined what works and what doesn't, the biggest limiting factors to collaborative relationships, and how industry participants commonly work around them.
2. *Identify the most important pain points.* We tied those pain points to elements of existing policy as well as currently proposed legislation. Our goal was to provide policymakers with an industry perspective on the problems of cross-border collaboration, illuminating the day-to-day challenges that businesses face.
3. *Provide concrete reform proposals.* From our survey outreach, workshops and program deep dives, we generated policy recommendations to maximise international cooperation and realise the strategic aims of AUKUS Pillar 2.

Policy recommendations have come and gone over the decades. Throughout that time, defence export-control and comparable rulebooks have been widely decried as an overbearing impediment to allies' cooperation in defence innovation, and a detractor for entrepreneurs who might otherwise seek business opportunities in the defence sector. Few reform proposals have been able to drive real progress.[10]

The will for change exists, but real change depends on operational realities that remain stuck in a legacy regulatory environment. Administrators default to doing it the way it's always been done. Politicians carve out exceptions for special interests. Everyone adds more rules rather than paring them back and simplifying them. Momentum dies somewhere between the national-security strategies and the codes of regulation.

Industry perspectives

Our 12 recommendations arise from ASPI's extensive engagement with private- and public-sector participants across the Australian defence industry. In the detailed recommendations made in this report, several overarching themes stand out:

- *Start from first principles.* Reform must begin with practical objectives, not with noses buried in rulebooks. The goal isn't to muddle through the labyrinth, identifying dead ends and devising paths around them. It's to imagine the best innovation system and then to design a collective regulatory system to facilitate its development. That requires looking at the system through the eyes of the businesses that must navigate it every day.
- *Consult and be transparent.* Regulatory authorities must do more than solicit input from an existing network of successful defence-industry participants. They must engage across the spectrum and identify practical impediments to compliance for businesses that haven't been successful or fortunate or have shunned defence opportunities altogether. They must do that in a variety of ways: online tools, industry forums and old-fashioned pressing the flesh at events inside and outside the traditional defence industry. They must openly parse industry criticisms and adopt a range of approaches to addressing problems.
- *The goal isn't just to make things possible, but to make them easy.* Just as important as simplifying, synchronising and streamlining the rules is creating a quick and easy means of compliance. The internet revolutionised the taxi industry with one basic online marketplace connecting drivers with riders. Tinder has done the same for the dating market! This should be the organising principle of AUKUS Pillar 2. Companies on unfamiliar terrain will need not only customers, advisory services and international partners, but also ways of connecting with them that are compliant by design.

Eight ITAR problems

William Greenwalt and Tom Corben of the US Studies Centre identify what they believe are eight key problems with ITAR that combine to stifle international cooperation in defence innovation:

1. An outdated mindset defaults to a lack of openness, even for close allies.
2. The definition of a 'defence article' is broad and fails to distinguish truly sensitive technologies.
3. Extraterritorial application is global and permanent, requiring approval by US authorities for any future transaction of exported products.
4. The rules don't distinguish between allies and adversaries; nor do they balance risk with potential gains.
5. Processes are inflexible and slow, applying standardised procedures divorced from operational needs.
6. Interaction with ITAR in any phase of development (known as 'ITAR taint') ties a product to the system forever.
7. The system doesn't acknowledge the capability of allies' export-control rules.
8. The unreasonable assumption of predictable, linear innovation demands that companies specify all activities in advance.

Reform as opportunity, or threat?

Australian businesses express concern that the strategy of 'expanding the ITAR bubble' to include the US's AUKUS partners could have the opposite of its intended effect. The Australian defence industry contains many SMEs lacking experience compared to US competitors in the areas of international trade and US Government contracting. Those SMEs face tight funding constraints and unpredictable cash flows, creating strong reliance on speed-to-market and the breadth of an international customer base.

Smooth trade relationships with nations beyond the AUKUS partnership are vitally important. As AUKUS-centred reform ties the Australian defence industry more closely to the US and raises trade barriers with the rest of the world, it risks eliminating critical sources of revenue while opening opportunities only in markets in which Australian SMEs will struggle to win. That could create an environment in which defence opportunities can be pursued only by relinquishing opportunities in other sectors that are easier to monetise.

US defence-focused businesses have long experience in navigating the complex requirements of the US State Department and Department of Defense (DoD). Despite their knowledge and experience of operating within the US system, they often complain about the US Government's onerous requirements on issues ranging from IP handling to information security protocols to simply identifying sales opportunities among the myriad purchasing agencies. If those working every day with the US acquisition system have trouble navigating it, we can assume that Australian organisations hoping to operate there will struggle more. American businesses may have more to gain from increased access to the Australian defence procurement system than the other way around.

Regulatory reform must therefore do more than remove barriers to trade. It must actively work to level the playing field. Australia must empower its businesses with the tools to navigate rules with which they're unfamiliar. That empowerment must include resources to adapt to the new competitive environment. Australia must actively advocate for them at the government-to-government level, both at the outset and on an ongoing basis. Otherwise, Australian SMEs won't be able to win against competitors that are heavily subsidised by US small-business support programs.

If each partner country sticks with historical tendencies to build walls around its own ecosystem of SMEs, AUKUS won't realise its objectives. Australia has a long way to go to catch up with US support mechanisms. In any scenario of tit-for-tat escalation of protectionist measures, Australia will quickly lose. A successful strategy would ensure that everyone has equal access to government-funded support mechanisms across the AUKUS partnership.[11]

Selected US defence industry support programs

1. The *Small Business Innovation Research* and *Small Business Technology Transfer programs* provide competitive awards to encourage SMEs to participate in defence-focused R&D.
2. The *Mentor-Protégé Program* facilitates partnerships between SMEs and experienced defence contractors.
3. The *Rapid Integration & Scaling Enterprise* is a vehicle for SMEs to provide innovative solutions for rapid insertion into acquisition programs.
4. The *Cybersecurity Maturity Model Certification program* ensures that defence contractors are compliant with information-protection requirements.
5. *APEX Accelerators* provide businesses with expertise necessary to pursue and perform under DoD contracts.
6. The *Defense Innovation Unit* accelerates the adoption of commercial and dual-use technology.
7. *Manufacturing USA* is a network of manufacturing innovation institutes operating as public–private partnerships.
8. The *Manufacturing Technology program (ManTech)* advances manufacturing technologies and processes through joint, interagency and public–private collaborations.
9. The DoD *Office of Small Business Programs* runs a range of programs providing sole-source and limited-competition contracts to businesses from historically disadvantaged groups, including:
   - woman-owned small businesses
   - service-disabled veteran-owned small businesses
   - historically underutilised business zones
   - small disadvantaged businesses.
10. The *8(a) Business Development Program* is a nine-year program providing firms owned by socially and economically disadvantaged individuals with training, technical assistance and set-aside contract opportunities.

Above all, the entire Australian Government must see itself as a partner with the nation's defence industry and seek out opportunities to help the industry win. It must focus on making things easy rather than just making them possible. It should become a more active partner in international data-sharing arrangements so that such arrangements don't become just another administrative hurdle. The government should facilitate technical assistance agreements so that planning a simple meeting doesn't take six months, and it should proactively look for problems and help devise solutions.

Australia's strategy must be to seek out impediments to success that lie beyond the headlines. 'Doing my job' won't be enough. The US, the UK and Australia may be close partners, but that partnership is based on fundamentally free-market principles in which the operative force is creative destruction. The Australian Government will be a key participant in that competitive environment. Its most important competitor will be the reigning world champion: the US Government.

The existence of strong and focused defence industries in economies smaller than Australia's gives hope that this challenge can be met. Government holds a unique role in growing a successful defence industry, more so than in any other sector. Leaders in the Australian Government must reflect on what shape the nation's industry should adopt to create a meaningful and competitive contribution to the AUKUS partnership. Its view must be informed by industry participants and investors. It must back its position with real resources—as a customer, a regulator and an investor.

Recommendation 1: Empower and resource DEC, DISP and similar organisations as critical agents of Australian competitive advantage.

Avoiding business-as-usual

Proposed regulatory reforms under the AUKUS umbrella focus on lowering technical barriers to trade. Whatever the rhetoric about collaborative R&D, discussion about the less visible enablers of such activities has been inadequate. The US National Defense Authorization Act and Australia's amendments to the *Defence Trade Controls Act 2012* address only the tip of the international R&D partnership iceberg.

A clear example of this is the 'sand-in-the-gears' effect of restrictions on technical data transfers. Development and production efforts require seamless sharing of supporting data. Existing government approval processes add months or years to joint projects. US legislation directs its relevant agencies to accelerate such transfers but leaves the mechanics of doing so up to follow-on regulation. Regulatory implementation has historically been the time when good intentions get derailed by vested interests and entrenched organisational incentives. Telling program administrators to go faster—even providing tools to do so—doesn't change the incentives encouraging excessive caution.

Another example of the gap between theory and practice is the sharing of classified information. The US builds high walls around its defence industry through classification requirements. For decades, the default classification level on newly generated data has been 'Not Releasable to Foreign Nationals' (NOFORN). Australian businesses from diverse backgrounds tell us stories about the time and effort invested in co-development with US partners only to see deals collapse when key system components were found to fall under NOFORN restrictions.

US legislation encourages its defence officials to improve on this. It directs the DoD to develop a plan that:

1. recommends modifications to foreign disclosure policies and processes
2. establishes an information-handling caveat specific to the AUKUS partnership
3. reduces the use of the NOFORN caveat
4. improves processes for the protection of privately held IP.[12]

Those changes are welcome, but their true value will be realised only in the hands of those implementing them. Organisational incentives driving broad acceptance will be critical.

Recommendation 2: Consider both public- and private-sector organisational incentives.

Australia appears to be equally on the back foot in facilitating industry access to classified information. ASPI's conversations with employees of the Defence Industry Security Program (DISP) unearthed no parallel reform programs or institutional awareness of coming changes.

Any serious effort to integrate AUKUS industrial bases must include some alignment and opportunistic improvement of DISP regulatory requirements and processes with the US's NISP.

The same applies for activities of the Australian Government Security Vetting Agency. We spoke with employees of a large Australian contractor providing infrastructure security and personnel vetting services. They, too, were unaware of any large-scale efforts to synchronise practices across the AUKUS partnership. A plan isn't worth the paper it's written on without both impetus for change and broad recognition and acceptance throughout the affected organisations. We've seen little evidence that either exists within critical agencies in both Australia and the US. Leaders in the US DoD have been talking for decades about the overuse of the NOFORN label. Little has changed. In the end, punishments for under-classification remain far more severe than those for over-classification. None of the proposed regulatory changes will address this fundamental misalignment of incentives.

What gets measured gets done. Process changes require rigorous metrics and efficiency audits, and public celebration of successes. The hardworking government employees who are the subject of so much criticism—through no fault of their own—must be recognised and rewarded for meeting concrete goals. We can't expect them to act on the broad and ambiguous principles that currently animate the conversation about ITAR reform.

Finger-pointing instead of fixing

One SME that we interviewed had referenced the DEC Forms and Portal to conduct an export self-assessment. Guidance from the portal suggested that an export licence wasn't required. More than two years later, the Australian Border Force (ABF) sent them two separate violation letters related to the sale.

The company took the letters to DEC, citing guidance from the DEC's portal. DEC admitted that its guidance was open to misinterpretation but placed responsibility with the ABF. The ABF refused to retract the letters absent guidance from DEC. Both agencies refused the offer of a three-way meeting to clear up the issue.

Their experience was, that despite agreement from officials on both sides that the company had been treated unfairly, everyone pointed the finger elsewhere and refused to retract the violation letters on their own authority.

Overconfidence can be as dangerous as hesitation. Australian policymakers must plan accordingly. In any endeavour as complex as international trade compliance, issues that no one has foreseen will arise. Government has a history of micromanaging wide-ranging industrial policy initiatives and achieving far less than it would have under more realistic assumptions about probable levels of efficacy. The secrets to success are flexibility, failing fast and iteration. We can't anticipate every roadblock in advance and mandate compliance with a foolproof master plan. If failed experiments in applied regulation can be used to effectively refine those flexible processes, then they should be celebrated.

ASPI's respondents provided many examples of obstacles that don't seem to be anticipated by sanguine regulatory authorities. Licence exemptions available through ITAR 126.4 can save up to nine months in government-to-government transfers of technology and associated technical assistance agreements. However, the Australian Government rarely works without industry partners. Each requires a re-transfer agreement, approval of which adds between four weeks and six months to a project's timeline. Normal turnover of Defence's embedded contractors becomes a constant drag on productivity, with each new employee waiting months for State Department approval to work with foreign military sales technical data. Export-licence requirements are weaponised to protect commercial interests, as when US prime contractors withhold the transfer of technical data to Australian companies wishing to respond to Australian sustainment or acquisition tenders (even for their own Australian entities, in many circumstances).

From the moment the first legislation is passed, governing bodies must be in place with broad authority to drive solutions to both defence-centred and interagency problems. Those problems will come fast and hard, both within and beyond the Pillar 2 technology areas that garner all the attention. Governing bodies must listen and adapt based on feedback from industry.

As problems arise, the government can't be caught flat-footed. Its ability to mediate disputes, dismantle roadblocks and mitigate unintended consequences must transcend departmental boundaries. It's difficult to predict when and where problems will arise. Policymakers must invest far more effort in planning for the unknown and ensuring that there are capacity and capability to address obstacles as they arrive. That means establishing pre-existing governance structures with deep expertise, visibility into key outcomes and power to make changes on the fly.

Recommendation 3: Establish expert-led governing bodies for AUKUS to manage ambiguity and surprise.

Winding back the clock

Proposed reforms will have unintended consequences for one class of export-control regulation that's seen significant progress in years past. That field is dual-use technology. The US has long taken criticism over the draconian nature of ITAR. Largely stymied in its efforts to radically rethink the system by legacy organisational structures, it has turned instead to leveraging a parallel system aligned under a different management structure. That system is the Department of Commerce's Export Administration Regulations (EAR).

The Australian list of controlled dual-use goods and technologies can be found in Part 2 of the Defence and Strategic Goods List. The list is similar to the US' Commerce Control List, which specifies technologies subject to the EAR.

That's where the similarities end. While the US has put extensive effort into moving less-sensitive technologies to the Commerce Control List and tailoring regulations to their lower sensitivity levels, Australia treats military-specific and dual-use goods as largely the same. Apart from minor differences in the handling of information transfers, both are governed by the same body of regulation.

What does that mean for the proposed AUKUS export-control reforms? The reforms have focused almost exclusively on aligning Australia's export controls with ITAR. Less remarked has been the fact that Australian dual-use technologies will, for the most part, be subject to the same rules.

The result will be to undo much of the progress made in loosening US rules to reflect the operational realities of dual-use technology. And yet another opportunity may be lost: that of reinventing the way the US, Australia and the UK together bring export regulation into the 21st century.

One example of how the US distinction works well, however, is the *de minimis* provision contained within the EAR. A particular product is swept up by the regulations only if controlled content rises above a threshold of total product value. No such exemption exists in Australian law.

What happens to an Australian business working with dual-use systems imported from the US under the *de minimis* exemption? All its work will be drawn back into an ITAR-like system. Foreign-national employees could be prohibited from touching the technology without a licence from DEC and the implementation of all the necessary standing compliance mechanisms. Inefficiencies will be introduced as participants game the system by, for example, using US intermediaries to export dual-use technologies to third-country recipients.

The growth of Australian defence industrial capacity demands drawing in participants from adjacent industries. The impact of the current approach will be to repel them. Addressing the handling of dual-use technologies is an urgent priority.

Recommendation 4: Implement a differentiated approach to regulating dual-use technologies.

Workforce

Our interviewees noted that the Australian workforce is a constraint on defence exports that goes far beyond DEC staffing. The nation is highly multicultural, making restrictions on deemed exports to broadly defined 'foreign persons' (all non-Australian citizens) a particular challenge.[13] Many companies operating in the dual-use space are unaccustomed to defence markets and export restrictions. They face a choice between losing a large percentage of their workforce or investing heavily in compliance systems and processes.

The Australian defence industry is small relative to the US market to which it will soon be more closely joined. Basic economic theory tells us that small markets and small populations have less room for specialisation. Experiences bear that out. In preparation for AUKUS and the associated

rule changes, some (mostly larger) businesses have engaged in a concerted effort to bring on more expertise in international trade and export-control law. The experience has been dispiriting.

The Australian workforce, they say, simply doesn't possess the required expertise. Even as the public debates the degree of assistance the government should provide to SMEs to smooth the transition to new export-control rules, those knowledgeable about the labour market claim that the discussion is immaterial. The expertise doesn't exist—certainly not in the volume that will be required.

Compounding the problem are cultural norms of Australian labour-market participation. Perhaps befitting an economy with naturally lower levels of specialisation, workers prefer to try different things, move around, and learn throughout their careers. That isn't necessarily a bad thing, but in a complex, dynamic field such as international trade, deep expertise is a requirement. Jacks-of-all-trades won't cut it. What Australia has in spades is creativity, dynamism and a desire to make a difference. That innovative entrepreneurship, however, hits a regulatory wall.

The body of international trade law is large, complicated and constantly changing. It involves deep networks of brokers, freight forwarders, shippers and innumerable complementary roles, each requiring deep understanding. Export-control regulation overlies all of that, determining how goods are marked, tracked, handled and monitored. Violations can carry criminal penalties.

New hires expect a quick training program on the associated rules. They envision a few days in a classroom, a checklist of standard procedures, and off they go. Few have the passion needed to spend a career becoming an expert on the subject. As one hiring manager put it, 'Australians are not defined by their jobs like Americans are.' Value judgements aside, such common Australian attitudes create problems in a niche field such as international trade compliance.

In ASPI's conversation with the Office of Defence Industry Support (ODIS), we requested the list of referrals that the office provides to SMEs seeking help with export-control compliance. That list contained four boutique consultancies and a reference to general guidance published by the Australian Industry Group. The consultancies in question agreed that demand for their services will far outstrip their ability to supply them.

Recommendation 5: Support industry as it builds required skill sets that are currently lacking in the Australian economy.

Case study 1: SYPAQ

The conflict in Ukraine has made SYPAQ, and its 'cardboard drone', a globally recognised brand. Simple as it may seem, the underlying technology—known as the Corvo precision payload delivery system (PPDS)—is at the forefront of innovation in autonomous systems development.[14] It's also one of many product offerings from a company that's rising to prominence as an important Australian systems integrator. SYPAQ partners closely with Defence on a wide range of capabilities beyond its line of Corvo autonomous systems, including digital services delivery, software engineering and tactical data-link design, installation and maintenance.

The company's PPDS is an illuminating example of the opportunities and pitfalls raised by export-control reform. Autonomous systems are transforming military strategy around the world and bringing ever closer the relationship between commercial and sensitive defence technologies. Western nations are realising not only the potential of such systems, but the degree to which they depend on supply chains that are deeply enmeshed with the economies of potential adversaries. The recent Sovereign Uncrewed Aerial System Challenge held by Defence's newly inaugurated Advanced Strategic Capabilities Accelerator focused on identifying domestic sources of drone technology to reduce Australia's reliance on foreign technologies such as those of Shenzhen DJI Sciences and Technologies Ltd, which is the world's largest producer of consumer drones.

SYPAQ brings together a range of technologies to empower its PPDS. Beneath the cardboard airframe is sophisticated hardware and software componentry making up a military-grade control and decision-making system delivered at minimum cost. By deliberately balancing cost-effectiveness and durability, it can precisely position a payload of up to 3 kilograms at a range of up to 100 kilometres for as little as A$5,000. The PPDS technical solution leverages AI, GPS and a variety of other sensors to provide added accuracy and resistance to countermeasures.

As with many of the Australian businesses we interviewed, SYPAQ relies on global sales to both military and commercial customers. A core discriminator for the PPDS system (which is export controlled) is that it can be modified to suit a wide range of purposes. The platform is payload-agnostic—a product strategy that ASPI saw employed again and again by Australian businesses that want to serve defence markets without being hobbled by strict export controls at home and abroad.

SYPAQ has been successful in navigating the export-control requirements and processes of DEC and the ABF. Program administrators are generally collaborative and responsive. They understandably err on the side of caution, using processes that are 'inconsistently timely'.

SYPAQ's global sales to military customers are enabled by investment in a network of authorised shipping entities specialising in defence goods. The company carefully monitors the validity of end-user certifications, facilitating interaction with Australian and international regulators to ensure the safety and security of its products.

The importance of managing the supply chain

SYPAQ is an important case study, since its growth program relies on customers and suppliers beyond the AUKUS partnership. The ability of Australian SMEs to maintain such business relationships was the most important concern for many of the companies in our study. SYPAQ's strategy for delivering advanced autonomous capabilities at low cost relies on sophisticated supply-chain management. Where it chooses to manufacture or source components depends on customer requirements and the delivery timeline.

For any given order of a defence-focused system, the lead time for export approval commonly ranges from eight to 15 weeks. The company makes use of that time by carefully managing a tailored manufacturing plan that optimises dynamic sources of supply at that specific time.

How long will various components require for fabrication? How far must they be shipped? Would it be better to buy them or manufacture them in-house? What are the political sensitivities of buyer and manufacturer host nations? What's the regulatory environment in which they operate? By thinking through such questions, the

company can optimise not only end-product delivery, but the long-term maintenance and sparing plan necessary to support future operations.

SYPAQ's competitive advantage is about far more than cutting-edge technology. It's about understanding global supply chains and the patchwork of laws governing them. In that context, the company sees AUKUS as potentially benefiting the defence industry in much the same way that the Five Eyes framework has facilitated the intelligence community's mission. Clearing roadblocks between close partners will open new markets and new opportunities to optimise customer delivery. The key to making the most of it is flexibility.

In the past, ITAR has made it more difficult for SYPAQ to incorporate US sources of supply or sell to US customers. Six-month approval timelines are not uncommon. AUKUS could potentially change that calculation, and SYPAQ consistently re-evaluates its go-to-market strategy accordingly. Globally sourced technologies can be cost-effective but are coming under pressure. As for many businesses operating in defence markets, adapting supply chains to account for geopolitical risk is critical. AUKUS could present a new opportunity by rebalancing cost considerations with supply-chain assurance. But there's more to it than national-security strategy; businesses must remain profitable.

Recommendation 6: Understand and account for the changing costs and benefits associated with industry supply-chain strategies.

Size matters

As a successful and growing medium-sized business, SYPAQ maintains relationships with smaller defence-focused companies. Our discussions revealed many areas where minor differences in scale create large differences in competitive advantage.

Growing companies benefit from the widespread desire to foster a new generation of Australian national champions. Their products regularly cross the desks of program administrators. Familiarity and understanding enable sound decision-making, especially for disruptive technologies and products in the challenging grey zone between military and commercial applications.

Regulatory reform must avoid the trap of declaring success over easy wins. If AUKUS is to succeed, administrators must focus not just on companies like SYPAQ, but on the hardest cases: the small Australian businesses with grey-area technologies that rely on day-to-day cash flow and fickle investors. As one respondent put it, 'Defence policy is very personal' for small companies. A three-week delay to an export approval can mean missing a mortgage payment on the family home.

AUKUS reform must do more than open a path to export markets; it must be a facilitator for businesspeople who lack the time and resources to make navigating export-control regulations their full-time job. DEC must actively build its network, reaching out to small businesses rather than simply posting notices on its website inviting input.

The Australian defence industry is reaching a critical point. More so than either of its AUKUS partners, it relies on a broad base of small businesses. Fostering and growing that base is where Defence must focus its attention. More complex rules favour larger businesses with the resources to maintain compliance and the networks to find help. Too often in the defence sector, a firm's expertise in navigating regulations can be a better source of competitive advantage than supplying the best product. If reform adds to the regulatory pile, Australia's SMEs—and by extension, its entire defence industry—will be hurt.

Recommendation 7: Don't focus on past winners or declare success over easy wins.

As they lose competitiveness against larger Australian defence contractors, those small businesses will be subjected to more competition from US companies with far more experience operating in defence markets. The probability of winning at home and abroad will fall as competition strengthens. Scarcely able to navigate challenging Australian defence acquisition processes, they'll have little chance of winning tenders from the US DoD.

With that one–two punch comes a third: already meagre R&D investment from Defence is being further limited by the transition from the old Defence Innovation Hub to the new Advanced Strategic Capabilities Accelerator. Many businesses report that investment from Defence in new capabilities has dried up, and that old commercial vehicles

are wound down before the new ones are operational. Innovation funding is declining at the same time as exporting is becoming more difficult, and new competitors are poised to flood the market.

And the hits keep on coming. Stricter export-control rules require investment in compliant business systems. Should Australian small businesses be investing scarce resources in core technologies or in network assurance, human resource management and business system upgrades? That's the impossible choice many will face. AUKUS presents both challenges and an opportunity to address these issues.

SYPAQ relies on the broad health of the Australian defence industry. Whatever success it has had, its leaders are concerned that problems like these will have important long-term implications for the business environment.

Case study 2: Hypersonix

To highlight the challenges that Australian SMEs face in navigating the international defence trade environment isn't to suggest that experiences are uniformly negative. Some of the most well-known companies to emerge from the Australian defence industry have done so through effective partnerships with international partners and the public sector.

SYPAQ and Hypersonix are two such companies. Hypersonix's SPARTAN engine is the world's first 3D-printed, fixed-geometry scramjet. Powered by environmentally sustainable hydrogen, the system can accelerate air-breathing aircraft to high Mach numbers in a range of applications. Its DART AE and Velos intelligence surveillance reconnaissance platforms provide test and demonstration capabilities, while the Delta-Velos Orbiter is a step towards sustainable, reusable space launch to low Earth orbit.[15]

Developing such advanced technologies requires broad collaboration. Examining the experiences of a company that's successfully done so highlights issues that will be critical to the broader success of the AUKUS Pillar 2 initiative. Hypersonix's growth path required navigating challenges in data sharing, information security and system certification, among others.

Relationships are needed to build trust and understanding: start early

The company learned early the vital importance of investing in the knowledge and professional networks needed to facilitate international collaborative relationships. One of its first efforts involved joint design studies with a US aerospace prime contractor specialising in airframes. With the goal of studying the feasibility of integrating SPARTAN into a new airframe, the small-scale collaboration planned to make use of the US partner's best-in-class airframe design modelling software.

At the time, Hypersonix was a relatively new company without the wide name recognition that it's achieved in recent years. The modelling software required for the technology-integration effort had both commercial and military applications. Primarily focused on the former, neither company anticipated the obstacles it would face in gaining approval for the project through the US Department of State's Directorate of Defense Trade Controls (DDTC), which is the organisation that administers ITAR.

The collaboration was ultimately derailed by DDTC's unwillingness to share world-class aerospace technology with the—at the time—small and little-known foreign company. The project was minor and not critical to Hypersonix's long-term health, but it was a wake-up call on the importance of export controls to international collaboration. As a result, the company strengthened its efforts to anticipate such problems and build the relationships necessary to avoid them.

Success breeds success. As hypersonic technologies have gained widespread attention and Hypersonix has gained respect in the industry, barriers have come down. Regulators at both DDTC and DEC recognise the importance of its work. Personal relationships have developed, enabling close collaboration and resulting in several agreements with US suppliers providing a path to selling Hypersonix capabilities abroad.

Hypersonix's experiences with DEC and DDTC have improved since the early days. It characterises their current relationships as close and collaborative. That isn't to say that processes move quickly. Careful attention is required to tick the right boxes in the right order, and to anticipate where problems will arise, but our interviewees felt that the system strikes a reasonable balance between protecting sensitive technologies and fostering collaborative relationships. They see AUKUS as an exciting opportunity to further lower the barriers.

Potential benefits of tighter export rules

Many of the businesses interviewed during ASPI's research viewed tighter Australian export-control rules as an unfortunate cost of facilitating defence-industry trade with the US. Hypersonix takes a different perspective, noting that Australian regulation more in line with international norms will of itself provide benefits.

Under the current system, tighter US regulations impose individual liability on those operating in international defence markets. Compliance with ITAR is strictly enforced, and violations carry criminal penalties. That means US businesses tend to err on the side of caution. Opportunities for international collaboration come with careful cost–benefit analysis. On the cost side of the equation is the possibility that a partner's mistakes will be met with severe penalties for US counterparts.

In that environment, large, successful US defence businesses see little upside potential in working with the relatively small and inexperienced enterprises so common in the Australian defence industry. The benefits don't outweigh the risks.

Bringing Australian export-control regulations up to parity with US law could thus provide benefits to help counterbalance the costs of operating under a stricter system. Australian businesses would be subject to the same restrictions as US counterparts in areas such as re-exports and deemed exports. They would be subject to similar criminal liabilities. Rather than US businesses assuming liability for the actions of a partner, Australian businesses would be responsible for their own actions in exporting joint technology projects beyond the boundaries of the AUKUS alliance.

That will change the cost–benefit calculations of US businesses. They'll be more willing to work with Australian partners since they'll no longer bear the cost of potential ITAR violations. Technology transfers to and from Australia will be licence-free, and whatever entity seeks to export to a third country will be responsible for compliance.

Tighter rules will also open opportunities within the domestic Australian defence industry. Hypersonix has conducted important R&D through partnerships with universities. Those relationships are limited by an academic security environment that isn't up to international standards. Were Australia to strengthen those security measures and make them comparable to the US system, Australian defence companies could make better use of resources available in academia.

Recommendation 8: Recognise that synchronised and simplified regulations are the key to success.

The critical need to align industrial security protocols

Discussions with Hypersonix about collaborative technology development highlighted several areas for improvement that came up repeatedly in our research. The first was industrial security standards. Australia's DISP is not only expensive and cumbersome for domestic use, but its lack of alignment with the US's NISP creates roadblocks for international partnerships.

The two nations' industrial security programs are critical to helping SMEs operate in defence markets. The security measures needed to develop and market military capabilities are stringent and expensive. Australia's DISP not only sets standards and provides advice to defence-industry participants, but it helps them to set up the secure facilities necessary for their operations.

But DISP can struggle in execution. Setting up a secure facility to enable work on classified systems can take 18 months or more, and costs can run well into the hundreds of thousands of dollars. The endeavour is beyond the reach of most Australian SMEs, effectively prohibiting them from working with the most important and sensitive technologies.

Further obstacles are created by differing standards between DISP and NISP. Even after an Australian business gains access to a secure facility, it may remain prohibited from working with controlled US technologies for several reasons. Not only might the DISP-approved facility not conform to NISP standards, but the means to share data via secure international channels are also lacking.

US industrial security standards supporting its defence industry, although far from perfect, are more developed than those in Australia. Most of the businesses ASPI interviewed, Hypersonix included, felt that Australia would benefit from relying far more on US standards, perhaps even working to integrate DISP and NISP under a single oversight entity. Australian and US industry would benefit both from standardisation and from the sharing of best practices.

Closer collaboration at the governmental level would have important benefits. Setting up a NISP-certified sensitive compartmented information facility (SCIF) is easier and

cheaper than its Australian equivalent, and the construct is far more flexible. Components of a broad enterprise can be walled off, tailoring the scale of the controlled environment to only what's needed.

SCIFs can be shared, or even set up by the government as incubators for resource-constrained SMEs to begin working with classified technologies. They can be established in university technology laboratories and, together with greater effort placed on joint security vetting, be a vehicle for expanding the research resources available to the defence sector.

Recommendation 9: Align Australian industrial security standards and data-sharing protocols better with the US system.

Certification processes must be a key focus area. They must be efficient, standardised and available at minimum cost. Embedded, continuously updated processes that account for rapid change in areas such as cybersecurity would have broad payoffs in enabling the type of industry collaboration envisioned by AUKUS planners. Such government investments would have large long-term payoffs.

The value of information sharing has been demonstrated through partnerships such as the Five Eyes intelligence arrangement. Expanding such concepts to incorporate technological development and enable broad industry participation will be a necessary enabler of the AUKUS Pillar 2 vision. Ongoing efforts to build a secure cloud environment must take on a new sense of urgency, and their scope should be expanded beyond direct support to military operations.

The ability of Hypersonix to grow and penetrate foreign markets is limited by lack of effective data-sharing standards. While export controls on hardware like SPARTAN are manageable, far more difficult are controls on the flow of data necessary to develop and share such technologies.

An important market for Hypersonix is the testing and demonstration of hypersonic systems. In that domain, Australia has an unmatched comparative advantage in the form of over-land test ranges. Most US hypersonic tests must now be conducted over water. That limits the ability of technicians to recover test vehicles and makes observation easier for adversaries. Capacity at test ranges is a critical limiting factor of US hypersonic system development.[16]

However, Australia can't capitalise on its advantage in over-land test ranges due to restrictions on data sharing. NOFORN classification of flight data encryption makes it nearly impossible to test US systems over Australia in vehicles incorporating Australian components. Data often passes through US satellites and incorporates US cybersecurity standards, further limiting international participation. AUKUS must address such barriers.

Broad alignment of technology standards

Late in 2023, the US Defense Innovation Unit signed a contract with New Zealand's Rocket Lab to launch Hypersonix's DART AE suborbital, hypersonic drone from Wallops Island, Virginia. Preparations for the launch have brought to light a host of challenges that must be addressed if AUKUS is to realise its full potential.

Technology standards that enable industry collaboration go far beyond the sharing of classified data. Hypersonix's core scramjet technology operates on hydrogen fuel. Hydrogen standards are different in the US and Australia, complicating its ability to refuel the vehicle during joint operations. Hardware certifications differ, magnifying the challenge of integrating Australian, US and New Zealand technologies. Conflicting standards for the use of the electromagnetic spectrum can cause interference between partners' communication and radar systems. And so on.

Comparing Rocket Lab's experience in planning for the Wallops Island launch with Hypersonix's experience is illuminating. Early on, New Zealand chose to emulate existing US regulations and standards for space-launch activities. That decision has contributed to the success of what's rapidly growing into a national champion. Rocket Lab is becoming a launch provider of choice for the US Government and is even expanding into adjacent markets.[17] Streamlining all the details that make such cooperation possible is an important part of its ability to collaborate across borders.

Recommendation 10: Ensure compatible technology standards with AUKUS partners to lower barriers to collaboration.

Case study 3: Mellori Solutions

Australia's industrial base consists disproportionately of small businesses. Defence's largest procurements are primarily awarded to US prime contractors or their regional subsidiaries. A few medium-sized Australian companies have carved out niches in critical capability areas, but the low level of domestic demand, a challenging Defence procurement environment and low public investment have left most defence-focused businesses starved for customers and growth capital. That's kept them small and highly reliant on global markets and dual-use technologies. This puts Australia in a vastly different position from both of its AUKUS partners, and especially the US.

That isn't for lack of innovative products and strong business plans. In fields ranging from autonomy to hypersonic vehicles, Australian technology is at the technological frontier. Mellori Solutions is one such company that moved early to fill a key gap in Australian defence capability.

Providing training, testing and technology services for the electromagnetic warfare (EW) systems of the ADF and its major partners, Mellori Solutions' capabilities fall squarely within the technology priorities of AUKUS Pillar 2. The company is a prime example of the kind of business that must be empowered by ongoing reforms if the AUKUS partnership is to succeed.

As small businesses go, Mellori Solutions is well placed to take advantage of partnership efforts. It's an Australian leader in a fast-growing technology area. Its business provides testing, maintenance and upgrade services to large users and providers of EW systems, fostering the kind of relationships that are critical to success. In addition to Defence, the company works closely with a range of multinational prime contractors. Nevertheless, the unique challenges of operating in the Australian defence industry restrict its ability to grow internationally.

Many of those challenges we've heard before. Reliance on technologies restricted by ITAR stifles the full range of products and services that Mellori Solutions can offer to its customers. Indeed, customers are often the problem, contractually mandating ITAR-free technologies to avoid the program delays that often go with them.

That forces the company into inefficient supply-chain relationships, including using 'good enough' components with lower capability or even sourcing from companies with geopolitical supply-chain risk because they're the only alternatives.

Looking at Mellori Solutions as a case study in export control is particularly informative due to the nature of its technology. Expertise in EW systems, unlike many other defence-oriented technologies, isn't concentrated in the US. Maintaining a leading position in the field requires working with organisations around the world, including enterprises in South Africa, Germany, Israel and Italy. In an AUKUS context, smoother relationships with US entities are unlikely to compensate for barriers raised to the rest of the world.

Not only must Mellori Solutions source equipment from global suppliers, but it also relies on a workforce drawn from those international centres of excellence. The 'big yard and high fence' envisioned by AUKUS planners will inhibit the development of two of Mellori's critical sources of competitive advantage: access to best-in-class technology and the people who make it work.

ASPI's discussions with Mellori Solutions employees brought to light many of the same concerns we've heard from others. Information flowing from Defence on the coming reforms—and what will be required to maintain compliance—has been thin. Partnerships with local prime-contractor subsidiaries such as Raytheon Australia's SME capability enhancement program have gone some way towards filling the knowledge gap, but such programs have been haphazard across the broader industry and have focused on narrowly defined areas of joint interest.

Success under the AUKUS framework will require overcoming such barriers. The initiative must identify technologies in which Australia can add value, pull in companies with those capabilities, and facilitate their efforts to win in international markets. It must acknowledge that some businesses will be unambiguously hurt by the rule changes. It must find ways to produce benefits that outweigh those costs.

Winning in the US acquisition system

In essence, AUKUS is about expanding the collective industrial and technological capability and reach of the three nations. The sum must be more than its parts. Yet none of the AUKUS countries began this journey at the same starting line. Australia has much to offer, and much to gain, but it must make up ground quickly. The core purpose of the AUKUS effort is to maintain stability in the Indo-Pacific, and Australia is the key nation in the alliance sitting squarely in the middle of the region. If Australia fails, everyone fails.

A critical enabler of Australia's success will be resilient and scalable industrial capacity that can respond to regional threats as they grow and change. Building that capacity will increase the depth of allied defence markets and add important areas of specialisation to fill gaps in allied capability. Increased dependence on US suppliers would be counterproductive to that objective.

Therefore, enhancing the ability of Australian businesses to sell into US markets is vital. Complaints about opacity and sclerosis in Australian procurement processes pale in comparison to the challenges that small Australian businesses face when they serve the US DoD.

Lacking the networks, know-how and citizenship required to compete successfully in most US defence procurements, Australian businesses wishing to sell there often start with Defence representatives at the Australian Embassy and various liaison offices embedded within US combatant commands, headquarters organisations and large programs like the US Air Force's Big Safari. Those points of contact facilitate discussions with US acquisition officials seeking relevant capabilities. For Mellori Solutions, the usual path is through US foreign comparison testing trials.

This business development process isn't standardised and relies on shifting networks of personalities and professional relationships. Defence's contribution to liaison activities is often not resourced to the necessary level, resulting in delays and missed opportunities. Even when it works as designed, it opens Australian businesses up to only a small slice of potential business available from the US Government.

Supporting US defence customers remains challenging even after opportunities are identified. Succeeding in that complex and highly regulated market requires many years of learning by doing, which is experience that few Australian businesses possess. US buyers will often ask Australian competitors to partner with US businesses to avoid the obstacles that come with inexperience.

Such partnerships have legal implications of their own, requiring separate contracts, IP agreements and narrower margins. There's broad agreement that succeeding in the long term means having the scale to run separate operations in the US. That objective is out of reach for many Australian businesses.

Recommendation 11: Prepare Australian industry to win in a new acquisition environment.

If the Australian Government is to realise the gains that it envisions from AUKUS, it must do far more to facilitate the participation of Australian businesses in the US market:

1. ODIS must have a significant presence at the Australian Embassy, managing a dedicated staff of business development professionals and DoD liaisons spread throughout the US defence system.
2. More people and resources on the ground are needed to jump-start the network-building that powers the US defence industry. Defence should establish permanent 'landing pads' on the east and west coasts for Australian companies seeking defence business in the US, including secure facilities integrated with those of US partners and access to embassy industry-support resources.
3. The government must provide training on US procurement practices and tools to connect Australian industry with opportunities in the US. That can be done both in Australia with experts hired specifically for the purpose and via a permanent ODIS presence in the US. Defence should provide consolidated and funded access to courses available through accredited providers and such US organisations as the Office of Small Business Programs and the Defense Acquisition University.
4. The government must level the playing field by pushing the US to open its small-business preferential contracting and grant programs to Australian participants. Defence must reciprocate for US businesses wishing to develop substantive capability in Australia.

Scaling up to compete in a larger market

Yet another important problem facing Australian defence businesses operating in the US is size. The DoD's total defence budget is nearly 25 times the size of Australia's. It employs more than 1.3 million active-duty service members, next to 77,000 in the ADF. When the DoD buys something, it buys a lot of it.

The US defence industry is commensurately large, with businesses that are more appropriately scaled to support the domestic level of demand. At the same time as Australian businesses struggle to win in an unfamiliar acquisition environment, they'll struggle to service the size of the requirements out for tender from US defence customers.

With success across the range of challenges identified above, that problem will naturally fix itself over the long term. The Australian defence industry will grow and adapt to fit the new circumstances. But, in the short term, the industry is poorly placed to scale up manufacturing facilities and expand supply chains to the necessary degree. The government must help industry adapt to the new challenge by facilitating the financing and partnerships needed for rapid growth.

An Australian business accustomed to receiving orders for a handful of units must be able to respond to an opportunity to sell thousands. It takes time and money to achieve that kind of scale, and customers won't wait. Mellori Solutions estimates at least $35 million in annual sales will be necessary for most Australian defence businesses to respond to common US procurement volumes. That's a high bar for an industry so dependent on small operators.

The problem has short-term and long-term solutions. In the short term, businesses may be able to secure contract manufacturing capability and alternative sources of supply. They can form partnerships or bid only on small portions of larger requirements (where acquisition strategies allow). But such approaches are expensive and limit growth potential. They rely on traditional Australian lending facilities that are less familiar with international defence markets and may hesitate to provide the necessary financing. Some approaches confront environmental, social and governance (ESG) restrictions on lending to the defence sector. The government must step in where necessary, providing incentives or direct support.

In the long term, SMEs will need to expand their organic capacity. That requires investment of a different sort: growth capital rather than short-term loans. Australian venture capital and similar sources of financing are small by international standards, amounting to only a 10th of the US total as a percentage of GDP in 2020, the most recent year for which data is available.[18] Policies to grow that funding pool and steer it towards the defence sector require careful attention to the investment business case.

Venture capitalists have other options. Those wishing to invest in the defence sector already face headwinds in the form of below-average profit margins among established participants.[19] That, along with ESG concerns and the risk profiles of innovative young companies, is likely to put off more stable sources of capital underpinned by Australia's massive superannuation funds.[20] Poorly designed or executed regulations implemented under the AUKUS banner will further decrease profitability, increase risk, and tip the balance towards adjacent industries without such onerous restrictions.

The government must help fill that gap directly as it creates incentives to encourage growth. Public–private partnerships take many forms in the US and have been successful in bridging such gaps.[21] Australia should benchmark against the wide variety of examples on offer, such as the US's Office of Strategic Capital, its Small Business Innovation Research program, and its model for federally funded research and development centres. At the same time, it must explore wider options for removing barriers to private-sector sources of funding.[22]

Recommendation 12: Support scaling up, which requires access to capital from both public and private sources.

Going beyond dual-use technology

Australian defence acquisition strategies—indeed, those around the world—make much of the importance of dual-use technology. That attention is well placed, as private-sector R&D funding is strongly outpacing similar public investments in many technologies relevant to national defence. The ADF and its partners must be equipped with the best commercially available technologies.

However, commercially available capabilities will be table stakes in any great-power competition. Much is made of the importance of commercial drones in the Ukraine conflict—but that conflict has reached a stalemate. Commercial technologies are quickly replicated and countered. Sustained military advantage comes from traditional classified defence R&D that happens behind barbed-wire fences and locked doors.

Participating in that R&D environment means having access to classified sources of information and secure collaboration tools. In this area, the Australian defence industry lags far behind. Mellori Solutions uses a remote-access system available from DISP that operates only up to the 'Protected' level. Access to the Defence Secret Network is far more restricted and costly, and beyond the means of most small businesses. Full capability would require using government facilities or a secure network connection from a distant access node—an investment that would be feasible only if it were funded directly by Defence. This is a significant limiting factor in the field of EW.

There are indications that the Capability Acquisition and Sustainment Group is exploring options to make secure cloud solutions available for defence industry participants. How that will function in practice remains to be seen. Will international sharing of classified data happen through a common hub, maintained and protected by Defence? Will certification requirements be aligned across the AUKUS partner nations? Will each partner achieve its stated goal of reducing the use of classification caveats that exclude foreign persons?

Such questions were raised repeatedly in our discussions. They need answers before companies like Mellori Solutions can participate fully in US defence acquisitions.

Conclusions

Making the most of the AUKUS partnership—turbocharging joint R&D and commercialising critical Pillar 2 technologies—will require new ways of doing business. Reform must finally dismantle the roadblocks that are widely acknowledged to inhibit cooperation. It must start from first principles, examining problems from the perspective not of legal scholars and program administrators but of those who must deal with such problems every day.

Reformers must maintain open channels of communication. They must do so not only when it's easy and familiar, but across the full range of Australian businesses that may be affected by the changes. The objective must be to make collaboration easy, not just to make it possible.

Process changes must focus on simplification and speed. The SMEs on which Australia's defence industry is based don't have the deep pockets and fat Rolodexes of the global prime contractors. They can't afford to wait months for export approvals. They can't afford to neglect core technological capabilities in order to invest in compliant business systems.

AUKUS provides both opportunity and challenge. The competition that it unleashes could bring Australia's defence industry to the forefront or it could crush the industry under the weight of the globe's biggest player. Which direction it goes depends on the ability of the Australian Government to enter the fray as an active partner with the defence industry and quickly address the problems that hold the industry back. The ballast and the balance that the UK brings to AUKUS is important in that regard.

Both countries must consider how this bilateral component can contribute to desired trilateral outcomes.

Notes

1 Richard Marles, Grant Shapps, Lloyd J Austin III, 'AUKUS defense ministers' joint statement', Department of Defense (DoD), US Government, 8 April 2024, online; Defence Department, 'Defence Trade Controls Amendment Act 2024: strengthening Australia's defence export control framework', Australian Government, 2024, online; Defence Department, 'Passage of priority AUKUS submarine and export control exemption legislation by the United States Congress', media release, Australian Government, 15 December 2023, online.

2 State Department, 'Myths and facts about US defense export controls: fact sheet', US Government, 10 July 2013, online.

3 'Breaking the barriers: reforming US export controls to realise the potential of AUKUS', US Study Centre, 17 May 2023, online.

4 Ted Bromund, Daniel Kochis, *How to expand defense trade cooperation between the US, the United Kingdom, Australia, and Canada*, Heritage Foundation, 26 April 2017, online.

5 State Department, 'Myths and facts about US defense export controls: fact sheet'.

6 Bryant Harris, 'Congress lays groundwork for AUKUS export control reform', *Defense News*, 23 March 2023, online.

7 Defence Department, 'Defence Industry Development Strategy', Australian Government, 2024, online.

8 Gregory Sanders, Andrew Philip Hunter, Rhys McCormick, Samuel Mooney, Daniel Herschlag, *National technology and industrial base integration*, Center for Strategic and International Studies, 9 March 2018, online.

9 William Greenwalt, *Leveraging the national technology industrial base to address great-power competition*, Atlantic Council, 23 April 2019, online.

10 Congressional Research Service, *AUKUS Pillar 2: background and issues for Congress*, US Congress, 20 June 2023, online.

11 Office of Small Business Programs, online.

12 'HR2670: National Defense Authorization Act for fiscal year 2024', US Congress, 2023–24, online.

13 See Defence Department, 'Defence Trade Controls Amendment Act 2024: strengthening Australia's defence export control framework', Australian Government, 2024, online

14 'Corvo autonomous systems', SYPAQ, 2024, online.

15 Hypersonix, online.

16 Director, Operational Test and Evaluation, *FY 2023 annual report*, DoD, US Government, 2023, online.

17 'Rocket Lab makes its defense prime debut with $0.5 billion contract to design and build satellite constellation for Space Development Agency', 8 January 2024, Rocket Lab, online.

18 *OECD Statistics*, online.

19 'Data', *Damodaram Online*, 2024, online.

20 *Global pension assets study 2023*, Thinking Ahead Institute, 2023, online.

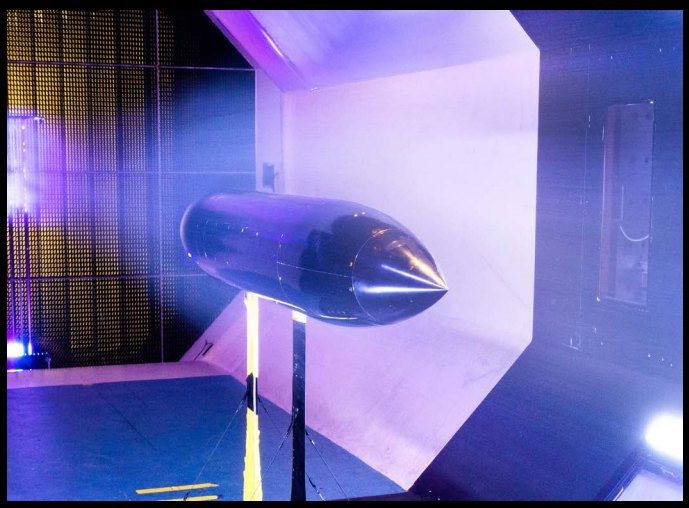
21 Bronte Munro, Gregory Brown, Nishank Motwani, 'Tapping the private sector to unlock AUKUS', *The Strategist*, 5 February 2024, online.

22 Hayley Channer, John Kinkel, *Upscale: Using private sector capital for the alliance*, US Studies Centre, 2024, online.

Acronyms and abbreviations

ABF	Australian Border Force
ADF	Australian Defence Force
AI	artificial intelligence
DDTC	Directorate of Defense Trade Controls (US)
DECO	Defence Export Control Office
DIDS	Defence Industry Development Strategy
DISP	Defence Industry Security Program
DoD	Department of Defense (US)
EAR	Export Administration Regulations (US)
ESG	environmental, social and governance
EW	electronic warfare
GDP	gross domestic product
GPS	Global Positioning System
IP	intellectual property
ITAR	International Traffic in Arms Regulations (US)
NISP	National Industrial Security Program (US)
NOFORN	not releasable to foreign nationals
ODIS	Office of Defence Industry Support
PPDS	precision payload delivery system
R&D	research and development
SCIF	sensitive compartmented information facility
SMEs	small and medium-sized enterprises

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE



ISSN 2200-6648