Journal of Strategic Trade Control
Vol. 2, December 2024

A missed opportunity: amending the Defence Trade Controls Act 2012 (Cth) and research security

Brendan Walker-Munro [*]

Abstract

Since the AUKUS Agreement was signed in 2021, there has been an ambitious reform agenda intended to align Australian export control laws with those of the US to ensure license-free exports of military and dual-use technologies upon which both Pillars of the AUKUS Agreement could be reliant. However, the Commonwealth government has missed a golden opportunity, by failing to contemplate how those export control reforms could be used to truly provide for safe and secure conduct of cutting-edge research in higher education institutions. The notion of "research security"—that is, "safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference"—appears to have been far from the minds of Parliament. This paper engages in a criticism of Australian export controls from the perspective of research security, highlighting aspects of the framework which fall short of protecting our institutions from malign foreign actors. Several recommendations are also made about potential opportunities for future reform that have broader application than just the Australian context and could be adopted by other jurisdictions looking to tighten their own research security frameworks.

Keywords
Australia, export control, higher education, national security, research security.

[*] Dr Brendan Walker-Munro is a Senior Lecturer (Law) with the Faculty of Business, Law & the Arts at Southern Cross University in Queensland, Australia. Brendan's expertise is in "research security", the use of law and policy to protect university research from national security threats such as espionage, foreign interference, hacking, and technology transfer. He also researches other aspects at the intersection of national security law and higher education, such as research funding, privacy, and digital security. Brendan is also appointed as an Expert Associate (Adjunct) of the National Security College at Australian National University and as a Senior Research Fellow of the Social Cyber Institute.

Article info

Submission date: September 17, 2024. Acceptance date: Noveber 21, 2024. Publication date: December 3, 2024.

How to cite
Brendan Walker-Munro, "A missed opportunity: amending the Defence Trade Controls Act 2012 (Cth) and research security", *Journal of Strategic Trade Control,* Vol. 2, (December 2024).
DOI: 10.25518/2952-7597.144

Publisher
European Studies Unit (ESU), University of Liège

Peer review
This article has been peer-reviewed through the journal's standard double-anonymous peer review, where both the reviewers and authors are anonymized during review.

Open access
The Journal of Strategic Trade Control is a peer- reviewed open-access journal. Accessible at www.jostc.org

Part I: Introduction

The imposition of control over what technology one country supplies another has been a key exercise of sovereign power, especially in the military domain. When a state has a technology that offers them military supremacy, transfers which benefit that state are frequently encouraged whilst transfers which undermine that state's superiority are condemned. It is in that context that the US, the UK, France, as well as Belgium, Luxembourg, the Netherlands and Italy originally formulated the Coordinating Committee for Multilateral Export Controls (COCOM).[1] The "gentlemen's agreement" at the heart of COCOM was succeeded by both multilateral export control agreements (such as the Missile Technology Control Regime, the Australia Group and the Wassenaar Arrangement, discussed below) as well as domestic export control frameworks,[2] of which the US has been infamously referred to as the most draconian regulations in the world.[3] Thus, it is striking that the US has (together with the UK and Australia) entered the strategic and technological cooperative security arrangement known as "AUKUS".

Constructed of two 'Pillars', the AUKUS Agreement enables the Royal Australian Navy to commence the building of a sovereign nuclear-powered submarine fleet (including the knowledge to construct, operate and maintain such vessels) together with strategic force enablement of the AUKUS partners through sharing of next-gen military technology: "artificial intelligence, cybertechnologies, quantum technologies" as well as undersea technologies and robotics.[4] As such, some scholars have suggested that the US has driven AUKUS with the goal gaining a stronger military presence (via its uplifted allies) in the Indo-Pacific region as a counter to the rise of autocratic states such as China and North Korea.[5]

---

[1] Cindy Whang, "Undermining the Consensus-Building and List-Based Standards in Export Controls: What the US Export Controls Act Means to the Global Export Control Regime," *Journal of International Economic Law,* 22(4) (2019), pp. 579, 584.

[2] Whang, "Undermining the Consensus-Building and List-Based Standards in Export Controls," pp. 585-588.

[3] Giovanna M. Cinelli, Kenneth J. Nunnenkamp, "Challenging Export Enforcement Actions: Policies of Denial under the International Traffic in Arms Regulations", *Global Trade and Customs Journal,* 8(7/8) (2013), p. 231; Kurtis J. Zinger, "An overreaction that destroyed an industry: the past, present, and future and US satellite export controls," *University of Colorado Law Review,* 86 (2015), p. 351; George Henneke, Roland Stephens, *AUKUS Pillar 2 critical pathways: A road map to enabling international collaboration*, Australia: Australian Strategic Policy Institute, May 2024.

[4] Michael Shoebridge, *What is AUKUS and what is it not? How does it connect to the Quad, the Sydney Dialogue, ASEAN and Indo-Pacific security?,* ASPI Strategic Insights, December 2021, p. 3.

[5] Shoebridge, *What is AUKUS and what is it not,* pp. 6-7.

The scope of sharing under the AUKUS Agreement is particularly astounding given the unusually restrictive limits on military technology transfers originating from the US. The International Traffic In Arms Regulations (ITAR) and the Arms Export Control Act of 1976 (AECA)[6] (including President Trump's Export Controls Reform Act of 2018)[7] specifically prohibits the transfer of articles and services related to technologies mentioned in the AUKUS Agreement from being transferred to Australia without a license, controlling the unauthorized export of 'defense articles' and 'technical data', as well as 'defense services' (i.e., anecdotally called the 'know-how' or 'know-why' of military and dual-use technologies).

This has direct implications for Australia's higher education industry. Australia has frequently linked its defense policy to reliance upon technological development to offset its small size and geographic isolation.[8] And much of the knowledge transfer behind uplifting of defense capabilities—both in terms of scientific knowledge and training of personnel—will occur at higher education institutions (HEIs).[9] Therefore, the sharply increased acceptance of increasingly sophisticated and/or classified military and dual-use technologies into these institutions will challenge their ability to keep those technologies protected.[10]

Numerous scholars and experts hypothesized how the sharing arrangements predicated by AUKUS could be implemented, including

---

[6] 22 U.S. Code 39.

[7] Contained within the *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115 232 (2018).

[8] Robert Wylie, Stefan Markowski, Peter Hall, "Big science, small country and the challenges of defence system development: An Australian case study," *Defence and Peace Economics,* 17(3) (2006), pp. 257-272; Peter Hall, Andrew D. James, "Defence Industrial Policies and Their Impact on Acquisition Outcomes: A Comparative Analysis of the United Kingdom and Australia," (Paper presented to the Defense Acquisition University Research Symposium, September 2012); Hannah Forsyth, "Post-war political economics and the growth of Australian university research, c. 1945-1965," *History of Education Review,* 46(1) (2017), pp. 15-32; Stefan Markowski, Rob Bourke, Robert Wylie, "Defence policy making: A case study of defence industry engagement in Australia", *Handbook of Business and Public Policy,* ed. Aynsley Kellow, Tony Porter, and Karsten Roni (Edward Elgar Publishing, 2021), pp. 215-231.

[9] Brendan Walker-Munro, Lauren Sanders and Rain Liivoja, "Preparing Australian universities for AUKUS," *The Strategist*, August 7, 2023, Australian Strategic Policy Institute, <https://www.aspistrategist.org.au/preparing-australian-universities-for-aukus/>.

[10] See for example: Parliamentary Joint Committee on Intelligence and Security, *Inquiry into national security risks affecting the Australian higher education and research sector*, Canberra, March 2022.

direct amendment of US export controls,[11] designating Australia as a 'domestic source',[12] the issue of a Presidential executive order,[13] or even an entirely new law throwing aside US export control.[14] Yet that legislative fix is now in. The 2024 National Defense Authorization Act for Fiscal Year 2024,[15] together with a broader licensing regime allowed under an interim final rule issued by the State Department,[16] has created obligations for the other AUKUS partners to be 'comparable' to the US ITAR before any transfers may occur.[17]

Australia has been reasonably quick to undertake just such agenda of 'comparability', completing both a statutory review of its export control laws together with a rapid tranche of legislative reform early in 2024. But did Australia miss out on taking steps that would have better secured its research ecosystem from national security threats? In other words, is the legislation protecting the right things? In my opinion, it does not, and the Australian government squandered a golden opportunity to introduce critical reforms to protect its HEIs

This paper therefore makes a critical contribution to both the existing export control and emerging research security literature. The paper will open in Part II by discussing the concept of research security, and its intersection with the laws of export controls. Part II will also examine certain aspects of HEI research which could pose (and have posed) difficulties for export control frameworks. Part III will then examine both US and Australian export controls in brief. That examination is necessary to provide essential context to the recent set of amendments to Australian export control laws compelled by the AUKUS Agreement. The paper will then (in Part IV) assess these amendments for missed opportunities to better secure the conduct of research in Australian HEIs. That Part will heavily reference both independent reviews of Australia's export control legislation (the Thom Review in 2018 and the Tesch and

---

[11] William Greenwalt, Tom Corben, *Breaking the barriers: reforming US export controls to realise the potential of AUKUS*, United States Studies Centre Report, University of Sydney, 2023.

[12] 50 U.S. Code § 4552(7).

[13] Brandon How, "ITAR exemptions for AUKUS should come via Biden executive order," *InnovationAus*, May 18, 2023.

[14] For example, see the Truncating Onerous Regulations for Partners and Enhancing Deterrence Operations (TORPEDO) Act of 2023, S. 1471 of 118th Congress (2023).

[15] National Defense Authorization Act for Fiscal Year 2024, S. 2226 of 118th Congress (2024).

[16] International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation Among Australia, the United Kingdom, and the United States, 89 Fed. Reg. 67270 (2024) (to be codified at 22 C.F.R. pts. 123, 124, 126).

[17] International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation, §6833(b).

Samuel Review in 2023). Finally, picking up on the findings in Part V, the paper will conclude with options for improvement of the security of HEIs research through the export control framework.

Part II: Research security and the introduction of export controls

Research security—within the scope of this paper—refers to actions for "safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference".[18] The regulation of research security takes different forms depending on the jurisdiction, but all research security frameworks currently being utilized involve "the Government, along with non-departmental public bodies…[c]ontrolling who can perform research…[p]roducing guidance on how sensitive research should be performed, stored and disseminated…[and] [r]estricting how research and research outputs are funded and acquired".[19] Research security has therefore emerged as a mechanism for controlling or regulating the 'who', the 'what' and the 'how' of involvement in HEIs research in the age of decaying, vulnerable or volatile geopolitical relationships.

Such controls are usually present but scattered across numerous statutes: for example, laws that protect the rights to intellectual property,[20] prohibit unauthorized dealings with trade secrets / espionage,[21] or maintain high standards of research integrity (i.e., enforcing existing obligations of disclosure around funding, conflicts of

[18] For this paper, I take the definition of research security from National Security Presidential Memorandum Number 33: Office of the US President, NSPM-33 Presidential Memorandum on United States Government-Supported Research and Development National Security Policy, January 14, 2021.
Office of the US President, NSPM-33 Presidential Memorandum.

[19] Alexis Brown, *What's next for national security and research?*, Final report, Higher Education Policy Institute, February 2022, pp. 15-16.

[20] Melissa Flagg, Autumn Toney, Paul Harris, *Research security, collaboration, and the changing map of global R&D*, CSET Policy Brief, Center for Security and Emerging Technology, 2021, <https://cset.georgetown.edu/wp-content/uploads/CSET-Research-Security-Collaboration-and-the-Changing-Map-of-Global-RD.pdf >.

[21] So Young Han, Hang Bae Chang, "Comparative Exploratory Research to Improve the Research Security System: Focusing on US Research Security Cases," *Journal of Society for e-Business Studies,* (2022) 27(1), p. 111; Kathleen M. Vogel, Sonia Ben Ouagrham-Gormley, "Scientists as spies?: Assessing US claims about the security threat posed by China's Thousand Talents Program for the US life sciences," *Politics and the Life Sciences,* (2023) 42(1), p. 32.

interest, etc.).[22] The effectiveness of these controls might remain open to serious debate, but they have nevertheless appeared in numerous jurisdictions with high-performing HEIs in the United States,[23] Canada,[24] China,[25] the United Kingdom,[26] and the European Union.[27]

As to precisely 'how' research security can be provided within such frameworks, the consensus in the literature is for approaches with multiple 'pillars' supporting legislative controls with policies around implementing those controls. For example, in the United Kingdom, a recent report by Universities UK International suggested that the government and institutions should focus on "six domains of risk: financial, reputational, academic freedom and freedom of speech, security, relationship and personnel management, and cyber, intellectual property (IP) and data management".[28] In the US, researchers must make disclosure statements relating to their employment, appointments and engagement in foreign 'talent recruitment programs', as well as their institutions supplying information to the government as well as performing due diligence on contracts, collaborative partners and funding bodies for all research they conduct[29]—higher risk research warrants a higher level of scrutiny and satisfaction that the research will be conducted with the US' interests in mind.

Export controls can therefore be a very powerful 'pillar' in providing research security because they regulate the security of exchanging

---

[22] Tommy Shih, "The role of research funders in providing directions for managing responsible internationalization and research security," *Technological Forecasting and Social Change,* 201, 123253, (2024).

[23] "Research Security", National Science Foundation, 2024, accessed 19 September 2024, <https://new.nsf.gov/research-security>.

[24] "Safeguarding Your Research," Government of Canada, accessed 19 September 2024<https://science.gc.ca/site/science/en/safeguarding-your-research>.

[25] Ingrid d'Hooghe et al., *Assessing Europe-China Collaboration in Higher Education and Research*, Report, LeidenAsiaCentre, 2018; Samantha Hoffman, *The Hong Kong national security law and UK academic freedom* Report commissioned for the British Association of China Studies, 2021.

[26] "Trusted Research," National Protective Security Authority, 2023, accessed 19 September 2024, <https://www.npsa.gov.uk/trusted-research>.

[27] Council of the European Union, *Council Recommendation on enhancing research security* [2024] 9097/1/24 REV 1.

[28] Universities UK International, *Managing risk and developing responsible transnational education (TNE) partnerships*, Final report, June 27, 2024; see also Gordon Long, *Safeguarding the Research Enterprise*, Report commissioned by JASON for the NSF, March 21, 2024, p. 2.

[29] *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development,* National Science and Technology Council, Subcommittee on Research Security, Joint Committee on the Research Environment, January 2022.

information, data, and physical items related to militarily relevant technologies. Unsurprisingly, there is a line of argument in the literature that export controls are not intended to be used for research security purposes, and in fact can damage the HEI environment if used for that purpose.[30] After all, within an academic environment, it is increasingly common for individual university researchers to cooperate across institutions at the highest levels to achieve research excellence. The academic environment is populated by numerous systems, measures and programs to demonstrate or predict a particular HEI's achievements in research.[31] Those HEIs then use these research-oriented metrics to demonstrate their contribution to broader society, and proof of need for future funding to continue those contributions.[32] Concomitant with those measures, academics routinely push back against regulation of their conduct of research, arguing that the need for open science trumps national or sovereign concerns,[33] that nationality is not a proxy for risk,[34] and that the nascent forms of academic freedom are owed to all HEIs irrespective of size, output or prominence.[35]

The disruptive nature of technologies considered under AUKUS, coupled with national security threats implicated by the need for research security, mean that domestic regulation of military and dual-use technologies will be crucial for research security for five reasons. Firstly, almost every

[30] Whang, "Undermining the Consensus-Building and List-Based Standards in Export Controls;" Nidhi Subbaraman, "US Universities Call for Clearer Rules on Science Espionage," *Nature,* 592(7855) (2021), p. 501; Claire Stalenhoef, Machiko Kanetake, Marijk van der Wende, *The Implications of the EU's Dual-Use Export Control Regulation 2021/821 for Universities and Academics* (Utrecht Centre for Regulation and Enforcement in Europe Working Papers, October 2022).

[31] Robert J.W. Tijssen, Alfredo Yegros-Yegros, Jos Winnink, "University-industry R&D linkage metrics: validity and applicability in world university rankings," *Scientometrics,* 109(2) (2016), p. 677.

[32] M. A. F. Santini, K. Faccin, A. Balestrin, B. V. Martins, "How the relational structure of universities influences research and development results," *Journal of Business Research,* 125 (2021), p. 155.

[33] E. William Colglazier, "The precarious balance between research openness and security," *Issues in Science and Technology,* 39(3) (2023), p. 87; Marcus Smith, Patrick Walsh, "Security sensitive research: balancing research integrity, academic freedom and national interest," *Journal of Higher Education Policy and Management*, 45(5) (2023), p. 495.

[34] Wilner, et al., "Research at risk: Global challenges, international perspectives, and Canadian solutions," *International Journal,* 77(1) (2022), pp. 26, 48; Diarmuid Cooney-O'Donoghue, "The Politics of STEMM Collaboration between Australia and China: National Security, Geopolitics, and Academic Freedom," *Asian Studies Review*, (2024).

[35] Erin N. Grubbs, "Academic espionage: Striking the balance between open and collaborative universities and protecting national security," *North Carolina Journal of Law & Technology,* 20(5) (2019), p. 235; Brown, *What's next for national security and research?*.

critical technology—and certainly most of those contemplated in the AUKUS Agreement—are dual-use in nature.[36] Secondly, 'list-based' controls simply do not possess the speed and flexibility to regulate technologies that emerge in contemporary markets. The failure of such lists in the medical and life sciences is often cited as exemplifying the challenges in taxonomic controls.[37] Thirdly, the external (i.e., non-governmental) funding of research at HEIs has spiked in the last two decades, both as a function of the increasing commercialization of universities but also a return on investment from the quality of academic pursuit that occurs there.[38] This has resulted in HEIs (and not just in Australia) being incentivized to 'push research closer to the "D-end of the R&D spectrum".[39] Fourthly, the make-up of HEI staff and student demographics has markedly shifted. Exchanges between universities are more and more recognized as contributing to research excellence, and industry placements for both students and tenured academics are becoming far more common.[40] Lastly, the geopolitical arena—once the *domaine reserve* of states—is becoming increasingly volatile and contested, with HEIs becoming both instruments and targets of state influence, with both benign and malign outcomes.[41]

So, the use of export controls will remain a key pillar of research security endeavors in HEIs.[42] Export control laws regulate not only physical items

---

[36] Lauren Sanders, "Australia's defense export control regime and critical technologies," *Journal of Strategic Trade Control*, Issue 2 (2024), p. 7.

[37] P. Millett, et al., "Beyond Biosecurity by Taxonomic Lists: Lessons, Challenges, and Opportunities," *Health Security*, 21(6) (2023), p. 521; Brendan Walker-Munro, "Virtual Labs and Designer Bugs: Generative AI, Synthetic Biology and National Security," *Journal of Law and Medicine*, 31(2) (2024), p. 353.

[38] V. Lynn Meek, Martin Hayden, "The governance of public universities in Australia: Trends and contemporary issues", *Taking Public Universities Seriously,* ed. Frank Iacobucci and Carolyn Tuohy (De Gruyter, Toronto, 2005), pp. 379-401; Helen Irvine, Christine Ryan, "The financial health of Australian universities: policy implications in a changing environment," *Accounting, Auditing & Accountability Journal,* 32(5) (2019), p. 1500.

[39] John Krige, "Regulating the academic "Marketplace of Ideas": Commercialization, export controls, and counterintelligence", *Engaging Science, Technology, and Society*, 1(1) (2015), p. 1-10.

[40] Tim Pitman, "The evolution of the student as a customer in Australian higher education: A policy perspective," *The Australian Educational Researcher,* 43 (2016), p. 345.

[41] Eugene Skolnikoff, *Research Universities and National Security: Can Traditional Values Survive?* (MIT Working Paper MIT-IPC-02-005, April 2002); Tommy Shih, Andrew Chubb, Diarmuid Cooney-O'Donoghue, "Scientific collaboration amid geopolitical tensions: a comparison of Sweden and Australia," *Higher Education,* 87 (5) (2024), p. 1339.

[42] Wilner et al., "Research at risk," p. 48; Samuel AW Evans, Walter D. Valdivia, "Export controls and the tensions between academic freedom and national security," *Minerva,* 50 (2012), p. 169; John Krige, "Regulating the academic 'Marketplace of Ideas':

and devices, but also intangibles such as research data, software or technical specifications. Further, there is the flexibility of how these lists are utilized in the overall control framework. For example, not only can the content of a list of technologies subject to export control be amended almost at will by a State, but so can a list that permits or prohibits the kind or classes of person who might handle or deal with those technologies. A person or entity may be prohibited from dealing with a given technology on any ground connected with reasons of national security, economic security or foreign policy, with few reasons needing to be given and appeals largely rare.

Part III: US and Australian export controls in brief

As outlined in one review of Australian export control law, "Australia needs a robust protective security system able to keep pace with a deteriorating global strategic environment… Australia's export control system is a central facet of ensuring this security".[43] Another review explicitly linked the protection of national security and foreign relations as a critical enabler for Australian defense and sovereign interests, because a failure to provide for adequate security would see Australia excluded from the 'club' of high-tech weapons providers like the US and UK[44]

In the context of the AUKUS Agreement, both Australia and the US have international obligations relevant to the trade in military technologies. For example, under the Arms Trade Treaty (ATT[45]) both states must regulate the trade in arms at "the highest possible common international standards" as well as ensuring their laws "prevent and eradicate the illicit trade in conventional arms and prevent their diversion."[46] Certain consensual arrangements—like the archetypal Wassenaar Arrangement, the origin of multilateral export controls on military technology[47]—also

---

Commercialization, export controls, and counterintelligence," *Engaging Science, Technology, and Society,* 1 (2015), p. 1; Mario Daniels, John Krige, "Beyond the Reach of Regulation? 'Basic' and 'Applied' Research in the Early Cold War United States," *Technology and Culture,* 59(2) (2018), p. 226.

[43] Senate Foreign Affairs, Defence and Trade Legislation Committee, *Defence Trade Controls Amendment Bill 2023 [Provisions]* (Final report, March 2024), p. 7.

[44] Vivienne Thom, *Independent Review of the Defence Trade Controls Act 2012*, Final report, 19 October 2018, p. 31.

[45] United Nations, Arms Trade Treaty, 3013 UNTS 52373, opened for signature 3 June 2013, entered into force 24 December 2014.

[46] ATT, art 1. I do note that the US signed the ATT but is not a Contracting Party.

[47] "About us", The Wassenaar Arrangement, accessed 17 September 2024, <https://www.wassenaar.org/about-us/>.

have a role to play. Certain 'non-standard' military items are usually regulated by such multilateral regimes, including the Australia Group on chemical and biological weapons, the Missile Technology Control Regime and the Nuclear Suppliers Group.[48]

US export controls

The US Arms Export Control Act (AECA)[49] grants the President authority over exporting 'defense articles and services', delegated to the Secretary of State to assess if the transfers enhance US security and promote world peace.[50] The authority of the AECA is then implemented by two parts of the Code of Federal Regulations, the EAR[51] and the ITAR.[52]

As mentioned above, ITAR is the US' main tool in regulating exports of defense technology. The genesis of the ITAR was in the Cold War, and it was primarily designed to service US defense and national security interests, whilst strictly controlling who could access US military technology.[53] The ITAR provides a robust platform for regulation by the Department of State of 'defense articles', 'technical data' and 'defense services',[54] and prohibits the export, re-export and transfer of those items without authorization. The specific 'defense articles', 'technical data' and 'defense services' declared by the President thus formulates the US Munitions List (USML) upon which much of the ITAR's regulatory controls are focused. What constitutes an export is incredibly broad—not only is actual exporting covered, but so is provision of technical data, transferring registration of articles, and performing acts of defense services.[55] So broad in fact are the deemed export provisions that a release of technical data to a "foreign person" is treated as an "an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency".[56]

---

[48] Christopher A. Ford, "Rethinking Multilateral Controls for a Competitive World," *National Security Law Journal*, 9 (2022), p. 225.
[49] 22 U.S. Code 2778.
[50] Executive Order 13637 of March 8, 2013, Administration of Reformed Export Controls, 78 FR 16127.
[51] 15 CFR §730-774.
[52] 22 CFR §120-130.
[53] Jason A. Crook, "National insecurity: ITAR and the technological impairment of US national space policy," *Journal of Air Law & Commerce,* 74 (2009), p. 505.
[54] 22 CFR §§120.2 and 120.10.
[55] 22 CFR §§120.50(a)(1)-(6).
[56] 22 CFR §120.50(b).

The Export Administration Regulations (EAR) on the other hand are regulated by the Department of Commerce, and control certain technologies which the Executive consider ought to be controlled in the interests of US technological supremacy, economic or foreign policy interests.[57] Under the EAR, exports of technologies are very broadly defined, such that the EAR describes the "release of technology to a foreign national in the United States through such means as demonstration or oral briefing is deemed an export."[58] A helpful view to distinguish the two is that the ITAR regulates 'traditional' military technologies that are usually forms of weaponry, whilst the EAR regulates dual-use technologies which are more readily identifiable as used in a civilian setting.[59]

The strict protections flowing from the ITAR and EAR have come at a price. US export controls laws are frequently cited as the number one obstacle to the proper implementation of AUKUS.[60] It has been suggested that the source of the overarching problems with the ITAR is the 'practical issues' associated with seeking, obtaining and maintaining export licenses as well as 'intangible, conceptual issues' said to hark back to the ITAR's Cold War heritage (where the US was locked in a strategic and technological battle for supremacy over Soviet Russia, a far different security environment to today).[61] At the same time, the EAR defines a dual-use technology to be "one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications",[62] capturing a massive variety of technologies. Indeed, these restrictions are said to be "particularly burdensome and inconsistent with the objectives of technology acceleration through AUKUS".[63]

Further, the US export control framework is largely decentralized and administered across numerous departments of the Federal Government.

---

[57] 15 CFR 730-774; authorized by the Export Control Reform Act of 2018 (ECRA).
[58] 15 CFR §730.5(c).
[59] Noting that on 9 March 2020, numerous firearms and ammunition were moved from the USML to the CCL: Control of Firearms, Guns, Ammunition and Related Articles the President Determines No Longer Warrant Control Under the United States Munitions List (USML), Federal Register 85(15), January 23, 2020.
[60] Greenwalt, Corben, *Breaking the barriers*; Tim O'Callaghan, Travis Shueard, Laura Coppola, "AUKUS, ITAR, Export Control Reform and the Australian Defence Industry", Piper Alderman, May 8, 2023, <https://piperalderman.com.au/insight/aukus-itar-export-control-reform-and-the-australian-defence-industry/>; Lauren Sanders, "AUKUS is supposed to allow for robust technology sharing. The US will need to change its onerous laws first," *The Conversation*, July 14, 2023).
[61] Greenwalt, Corben, *Breaking the barriers*, p. 10.
[62] 15 CFR §730.3.
[63] *Maximising Australia's AUKUS Opportunity,* PriceWaterhouseCoopers, AmCham, Australian-British Chamber of Commerce, Report, 2022, p. 27.

Although this paper deals only with the ITAR and EAR, the issues identified have broader implications. Whilst the US export control regime has a longstanding legal history, it has also been repeatedly reformed in the last decade to ensure the regulations "[a]s a matter of legal authority…apply to the transfer of specific or general types of technology to foreign persons…[and] their reach is not limited by law to a prescribed set of commercial circumstances".[64]

Australian export controls

Australia's contribution to international compliance with arms controls, and its principal form of regulation, is the Defence Trade Controls Act 2012 (Cth) ("the DTCA").[65] The DTCA operates as a blanket prohibition of supplying or dealing in 'DSGL technology' without license, being anything included on the Defence Strategic Goods List (DSGL).[66] The DTCA regulates the intangible supply of DSGL software and technology, brokering of DSGL goods and technology, and publication of DSGL technology. From the perspective of US military technology, the DTCA also gives force to the Australia-US Defence Trade Cooperation Treaty.[67]

The principal restriction in the DTCA was (prior to the passage of the amendments discussed below) entirely hinged on DSGL technology being 'supplied'[68] by a person without Ministerial approval in circumstances where such approval was required,[69] in contravention of the conditions of such approval,[70] or in contravention of a notice prohibiting that supply *ex ante*.[71] Other prohibitions applied for goods covered by the Defence Trade Cooperation Treaty,[72] or items on the DSGL dual-use list.[73]

---

[64] Mario Mancuso, *Modernizing Export Controls: Protecting Cutting-Edge Technology and U.S. National Security* (Testimony to the Committee on Foreign Affairs, 115th Congress, Second Session, March 14, 2018), pp. 3-9.
[65] See also the Defence Trade Controls Regulation 2013 (Cth).
[66] See s 112(2A)(aa); currently the Defence and Strategic Goods List 2021 (Cth).
[67] "Treaty between the Government of Australia and the Government of the United States of America concerning Defense Trade Cooperation", signed 5 September 2007, entered into force 16 May 2013; DTCA, s 4 and Pt 3.
[68] Whether by sale, exchange, gift, lease, hire or provision of access: DTCA, s 4.
[69] DTCA, s 11.
[70] DTCA, s 13.
[71] DTCA, s 14.
[72] As either an 'Article 3(1) US Defence Article' or an 'Article 3(3) US Defence Article': DTCA, ss 4 and 31.
[73] DTCA, ss 4 and 32.

In 2018, Dr Vivienne Thom completed a statutory review of the DTCA (the Thom Review).[74] That review found multiple gaps in the regulatory coverage of the DTCA, complexities in interpretation, and a general difficulty in both the administration and compliance with export controls.[75] One of the most significant problems identified in the Thom Review for Australian export controls was that the DTCA did not require a permit for certain exchanges of information or technology.[76] One submitter to the Thom Review asked "what precludes an Australian entity from simply arranging an overseas trip and providing access instead of seeking an intangible supply permit?."[77] That finding has implications for research security because the definition neatly applies to a common form of collaboration between academics—the sharing of intangible knowledge in overseas settings, such as at research conferences or during joint or multinational research ventures.

This led the Thom Review to conclude that substantial reform was necessary to bring Australia's export controls up to date with a rapidly shifting global scientific and technological research agenda—in essence, this was also an argument to enhance Australian research security. The Department of Defence proposed that it could notify a person that some technology they were dealing with "is significant to developing or maintaining national defence capability or could be used to prejudice the security, defence or international relations of Australia."[78] That person could then be required to apply for an export permit, even if the technology was not listed in the DSGL. That proposal was roundly criticized by industry and academia as creating imbalances between national security and international trade, would jeopardize international collaboration, lacked scrutiny and transparency, and came with increased complexity and cost.[79]

Instead, the Thom Review proposed nine recommendations: three with respect to improving the administration of export control licenses and interpretation of the DSGL, four with regard to addressing the legislative coverage of 'emerging and sensitive military and dual-use technology' (including the application of general monitoring and investigation powers for Defence[80]), one related to cryptographic controls, and one related to employees of Australia's nuclear science agency.[81] The Government

[74] Thom, *Independent Review*.
[75] Thom, *Independent Review*, pp. 5-8.
[76] Thom, *Independent Review*, p. 32.
[77] Thom, *Independent Review*, p. 33.
[78] Thom, *Independent Review*, p. 35.
[79] Thom, *Independent Review*, pp. 36-39.
[80] i.e., the triggering of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth).
[81] Thom, *Independent Review*, p. 5-8.

supported all nine recommendations,[82] yet no amendments to the DTCA had been undertaken by the time Australia announced the AUKUS Agreement.

Necessary amendments

The position Australia found itself in at the time of enacting AUKUS in 2021 was to align its export controls with those of the US and provide a "comparable" environment for the receipt of advanced military and dual-use technologies.[83] This was a complete reversal of direction from the findings of the Thom Review, which found that comparison of the US and Australian export control systems "was not possible or useful because of the inherent differences in the systems and the complexity of the US system."[84] Instead, Australia was now required to have a system directly comparable for AUKUS to work.

Reform was also "essential" for AUKUS because under both the ITAR and EAR Australia and the UK occupied the same level as countries non-allied to the US (such as Latvia[85]). That should be surprising, given that—for example—Australia is a partner (alongside New Zealand, Canada, the UK and the US) in the National Technology and Industrial Base, a statutory body designed to facilitate US national security outcomes by supporting "advanced R&D and systems development" amongst the member countries.[86]

How then did Australia tackle the amendment of its export controls in the face of AUKUS?

On 29 August 2023, the Australian Government appointed Peter Tesch and Professor Graeme Samuel to conduct the next statutory review of the DTCA (the Tesch/Samuel Review).[87] However, whilst AUKUS was not

---

[82] "Government Response to the Defence Trade Controls Act Review," Department of Defence, accessed 15 September 2024, 2018, <https://www.defence.gov.au/about/reviews-inquiries/defence-trade-controls-act-review-2018>.

[83] 22 U.S. Code 2778(j)(2).

[84] Thom, *Independent Review*, pp. 26, 49, 51 and 53.

[85] Thomas Corben, "AUKUS: A Year On. What to make of AUKUS after 365 days?," *United Service,* 74(2) (2023), pp. 13, 15.

[86] 10 U.S. Code §4801. See also Congressional Research Service, *Defense Primer: The National Technology and Industrial Base* (Report, March 30, 2023), <https://sgp.fas.org/crs/natsec/IF11311.pdf>.

[87] Peter Tesch, Graeme Samuel, *Independent Review of the Defence Trade Controls Act 2012* (Final report, December 15, 2023).

specifically mentioned, the Minister for Defence did note that the Tesch/Samuel Review would "evaluate the Act in the context of other reforms the Government is considering to defence trade". Curiously, before the Tesch/Samuel Review was concluded, the Defence Trade Controls Amendment Act 2024 (Cth) ("DTC Amendment Act") was introduced into Parliament on 30 November 2023, with the objective of amending the DTCA to provide for AUKUS. On its introduction, the DTC Amendment Act was referred to the Senate Standing Committee on Foreign Affairs, Defence and Trade (Senate Committee), in effect creating two separate lines of review of Australian export controls.

These reviews revealed numerous concerns with the reach and scope of the DTC Amendment Act. Submissions to the Senate Committee focused on the "shortness in time to consider the implications of what is a complex bill and that certain proposed measures have the potential to restrict international research collaboration".[88] Concerns were expressed about "inadvertently impact unaware university academics and researchers who routinely engage in research and publication without necessarily having full awareness of the Act's definitions and restrictions with regards to intangible supply."[89] Concerns were also raised with the lack of a 'basic scientific research' exemption, which submitters considered should have been aligned more closely to the US ITAR's fundamental research exemption (FRE).[90] Finally, and highly relevant to the topic of this paper, issues were identified with the 'increasingly complex compliance burden' faced by universities,[91] such that a single project could involve engagement with export controls, foreign arrangements,[92] the Defence Industry Security Program (DISP)[93] and Departmental guidelines on countering foreign interference.[94]

Despite the gravity of some of the concerns raised, both the Tesch/Samuel Review and Senate Committee review largely dismissed them. The Senate Committee in particular claimed "[t]he test for the bill is whether it strikes the optimal balance between national security and

---

[88] Senate Standing, *Defence Trade Controls Amendment Bill 2023*, p. 7.
[89] Tesch, Samuel, *Independent Review,* p. 8.
[90] Tesch, Samuel, *Independent Review,* p. 11.
[91] Tesch, Samuel, *Independent Review,* p. 11.
[92] Because of the Australia's Foreign Relations (State and Territory Arrangements) Act 2020 (Cth).
[93] "Defence Industry Security Program," Department of Defence, 2023, accessed 14 September 2024, <https://www.defence.gov.au/business-industry/industry-governance/defence-industry-security-program>.
[94] *Guidelines to counter foreign interference in the University Sector,* Department of Education, November 17, 2021, <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector>.

international trade and research collaboration. Viewed in this light, concerns voiced by stakeholders are largely centered on perceived unintended consequences."[95] What recommendations it did make were modest, and ironically reminiscent of most of the Thom Review's recommendations from 2018.[96] Other members of that Senate Committee were not so convinced, issuing a dissenting report that expressed the view that "[i]n a moment of genuine political irony this Bill, which is touted as part of Australia's national security response to a less certain world, will in fact make Australia less safe and will stunt academic and economic growth".[97]

Irrespective of those issues, the DTC Amendment Act progressed extremely swiftly, passing both Houses of Parliament on 27 March 2024 (a mere two weeks after the Senate Committee report) and receiving Royal Assent on 8 April 2024. The amended provisions of the DTCA took effect on 1 September 2024,[98] with a further 6-month "transitional period" (on or around 8 April 2025) during which new and modified offences under the DTCA cannot be prosecuted. In essence, the DTC Amendment Act has only changed the DTCA in three ways: by uplifting the 'basic research' exemption out of the DSGL and into primary legislation, creating new criminal offences relating to supply of DSGL goods or services to foreign nationals, and providing a national exemption to the UK and the US from Australia's export control permit requirements.[99]

Part IV: Missed opportunities? The DTCA and research security

The DTCA has always applied to academics and the conduct of research in Australia's HEIs, and so has the legislative basis and regulatory ambit to play a critical role in the provision of research security by limiting or eliminating unwanted technology transfers.[100] This is especially so given

---

[95] Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* p. 8.
[96] Tesch, Samuel, *Independent Review;* cf. Thom, *Independent Review*.
[97] Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* p. 26.
[98] Defence Trade Controls Amendment Commencement Proclamation 2024 (Cth).
[99] Similar exemptions were adopted by our AUKUS partners, with the US publishing an interim rule, and a similar "Open General Licence (OGEL)" for exchanges originating out of the UK: Bureau of Industry and Security, Export Control Revisions for Australia, United Kingdom, United States (AUKUS) Enhanced Trilateral Security Partnership, 89 FR 28594 (April 19, 2024); Department for Business and Trade, Notice to exporters 2024/09: update on AUKUS, May 1, 2024.
[100] Wilner et al., "Research at risk," p. 48.

that a significant proportion of intellectual capital that will be generated and utilized because of AUKUS in Australian HEIs.[101]

Anecdotally, academics have a historical and cultural issue with the adoption of security measures.[102] Concerns raised by academics and the HEI sector regarding export controls are usually not framed around proper uses of research security to protect our institutions; instead, submissions are usually concerned with projected impacts on academic freedom, international collaborations, and exchanges with foreign nationals.[103] Indeed, most of the submissions to the reviews of Australian export controls related to excluding as much HEI research as possible through the 'basic research' exemption.[104]

When the DTC Amendment Act was introduced into Parliament, the Defence Minister Richard Marles indicated that the Act would "bolster Australia's national security and protect our sensitive defence goods and technology."[105] Indeed, the Minister's comments made clear that the export control framework was *specifically* intended to provide for research security, saying "Australia's export control system is a key element of our protective security framework" and "[the Act] seeks to improve the government's ability to protect our sensitive defence goods and technology… tasks [that] are central to preserving Australia's national security and to keeping Australians safe."[106] But did the DTC Amendment Act achieve those lofty goals?

I submit that it did not. The amendments to the DTCA were undertaken with the sole purpose of meeting "comparability" with the US ITAR and with the political objective of advancing AUKUS. The opportunity for amendments to Australian export controls that could have achieved Minister Marles' grand policy statements (and thus enhanced Australian research security) has been squandered. The following Part expresses

---

[101] Peter Dean, Sophie Mayo, Alex Favier, *The university sector's value proposition for AUKUS: Times Higher Education Summit outcomes report*, Report, United States Studies Centre, March 2024.

[102] Ivano Bongiovanni, "The least secure places in the universe? A systematic literature review on information security management in higher education," *Computers & Security,* 86 (2019), pp. 350-357.

[103] For example, see Thom, *Independent Review,* pp. 36-39; Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* pp. 11-13; Tesch, Samuel *Independent Review,* pp. 1, 5-8.

[104] Thom, *Independent Review,* pp. 49-51; Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* pp. 8-11; Tesch, Samuel, *Independent Review*, pp. 10-11.

[105] Commonwealth, *Parliamentary Debates*, House of Representatives, 30 November 2023, 8923 (Richard Marles, Minister of Defence).

[106] Commonwealth, *Parliamentary Debates,* 8923.

numerous concerns with the current iteration of the DTCA through the lens of research security. Some of those concerns are quite grave, as they carry the potential to undercut the purposes of the DTCA to provide for security of our research institutions (which overwhelmingly are Australian HEIs). For others, the gravity of the concern hangs upon the interference (however unintended) occasioned by the DTCA provisions in the pursuit of academic inquiry, and the protections of academic freedom such pursuit invokes.

Fundamental research exemption (FRE)

Prior to the amendments in the DTC Amendment Act, universities were often in an invidious position because they could be obligated to seek a permit for the purposes of exporting information to foreign researchers, because the DTCA prohibited exchanges of DSGL information or technology between Australian-based researchers and foreign nationals. The Thom Review did not believe that a FRE was required in Australian export control,[107] a position reversed when both the Senate Committee and the Tesch/Samuel Review completed their reports.[108]

This was purportedly addressed by the introduction of a FRE into the DTCA.[109] Anything "produced in the course of" or "for the purposes of" such "fundamental research" is excluded from the definition of DSGL technology.[110] Such research can be either "basic or applied", but must be conducted in circumstances that meets the conditions of both "being intended for public disclosure, or would ordinarily be published or shared broadly", and "not subject to any restrictions on disclosure (however imposed) for purposes connected with the security or defence of Australia or any foreign country." Australia's definition draws contextual similarities to—but is distinct from—the exemptions in the ITAR (which exempts "research in science, engineering, or mathematics" which are published and not subject to restrictions "for proprietary or national security reasons")[111] and the EAR ("basic and applied research in science

---

[107] Thom, *Independent Review*, pp. 49-51.
[108] Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* pp. 8-11; Tesch, Samuel, *Independent Review*, pp. 10-11.
[109] DTCA, s 4 (definition of 'fundamental research').
[110] "DSGL technology means a thing that:
(a) either:
(i) is technology, as defined in the Defence and Strategic Goods List, *not including such technology that has been produced in the course of, or for the purposes of, fundamental research*…" (emphasis added); DTCA, s 4.
[111] 22 CFR §§120.34(a)(8) and 120.43.

and engineering where the resulting information is ordinarily published and shared broadly within the scientific community").[112]

The link between the FRE and research security is not clear cut. Put simply, research that falls into the FRE is exempt from export controls, meaning any attempt to secure it must be made using another 'pillar' of research security, i.e., migration restrictions, university policy, banned entity lists, etc. Thus, the breadth and scope of an FRE can determine how much and what types of research will need to be secured, and how, by each HEI.

In that context, three criticisms may be made about Australia's research exemption. Firstly, the Australian FRE differs slightly in language from its US equivalents in both the EAR and ITAR.[113] The difference is subtle, but hinges on the treatment of proprietary research. Consider for example the following scenario: a researcher is developing a new form of metamaterial. Such a metamaterial possesses new characteristics and significant commercial value. The researcher chooses not to publish their results to protect their intellectual property. Where that researcher is based in a US HEI, the FRE under both ITAR and EAR will not apply as the researcher has 'accepted' a restriction on publication for proprietary reasons. The Australian researcher on the other hand has conducted research that ordinarily would be published, but the restrictions on publication are not recognized by the FRE. Thus, the research remains exempted from the DTCA and may be shared with whomever the researcher wishes, creating massive issues for research security.

Secondly, the FRE is only triggered where outcomes of research "are intended for public disclosure, or would ordinarily be published or shared broadly."[114] The FRE therefore does not cover research not intended for public disclosure for reasons connected to the technology's novelty or economic interest, rather than its military utility.[115] Under Australian law, every employee owes their employer a common law duty of confidence (i.e., to keep secret the operations of the business),[116] so arguably *every*

---

[112] 15 CFR §734.8

[113] 15 CFR §734.8(a) and 22 CFR §120.34(a)(8).

[114] DTCA, s 4.

[115] Such as patentable research: Rochelle C. Dreyfuss, Jane Nielsen, Dianne Nicol, "Patenting nature—a comparative perspective," 5(3) (2018), *Journal of Law and the Biosciences,* p. 550.

[116] *Robb v Green* [1895] 2 QB 315; *Commonwealth v Fairfax* (1980) 147 CLR 39. Failures to uphold that duty could be subject to a claim of equitable breach of confidence, per *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41; approved in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

piece of HEI research could be seen as confidential.[117] That position is unlike the US, where publication guarantees form standard parts of research contracts.[118]

Thirdly, the DTCA limitation is far wider than the text in the ITAR, where universities must either "accept restrictions on publication of scientific and technical information resulting from the project or activity" and/or be funded by the US government where "specific U.S. Government access and dissemination controls" apply.[119]

On the one hand, the DTCA provision does not require the capitulation of the researchers or their HEI (as in the ITAR, where the researchers must 'accept' limitations), and allows the Australian government to impose arbitrary obligations on any research in the interests of the security or defense of Australia. On the other hand, there is no requirement on the government to demonstrate that any Australian interests would trigger the imposition of restrictions. As neither 'defense' nor 'security' of any foreign country is defined in the DTCA, restrictions could be imposed with regard to espionage, sabotage, politically motivated violence, promotion of communal violence, defense, acts of foreign interference and the protection of territorial and border integrity from serious threats. Imagine if an Australian researcher was collaborating with colleagues in Hong Kong on what would be captured by the FRE of the DTCA.[120] If China arbitrarily imposed national security prohibitions on that work, the wording of the DTCA would essentially 'pick up' those restrictions—because they are now "restrictions on disclosure (however imposed) for purposes connected with the security or defence of…any foreign country."

Emerging technologies and Part 2 of the DSGL

As discussed earlier, the DTCA continues to rely upon the DSGL as a statutory instrument to control a taxonomic list of technologies deemed to have either solely-military use (DSGL, Part 1) or potential dual-use (DSGL, Part 2). That reliance should be viewed as surprising, given that since 2018 the Australian Government has been on notice that the DTCA

[117] See generally *University of Western Australia v Gray* [2009] FCAFC 116; (2009) 179 FCR 346.
[118] Robert Kneller, et al., "Industry-university collaborations in Canada, Japan, the UK and USA–With emphasis on publication freedom and managing the intellectual property lock-up problem," *PloS One,* e903029 (3) (2014),; cf. Joshua Yuvaraj, Rebecca Giblin, "Are contracts enough?: An empirical study of author rights in Australian publishing agreements," *Melbourne University Law Review,* 44(1) (2020), pp. 380-423.
[119] 22 CFR §§120.34(a)(8).
[120] Hoffman, *The Hong Kong national security law*.

was no longer 'fit for purpose' in controlling the dissemination of dual-use technologies.[121] Submitters to the Senate Committee were concerned that Australia's laws risked less clarity than those of the US,[122] whilst submitted to the Tesch/Samuel Review lamented that five years on from Thom's recommendations, the DSGL retained the same level of ambiguity, where it was noted that the DSGL remained notoriously difficult to interpret.[123]

It is axiomatic that under AUKUS, both Australian HEIs and industry partners will conduct a range of research activities that will be implicated by Part 2 of the DSGL.[124] When conducting those activities, the risk of foreign influence or interference is a live one, and requires the Australian government focus reform efforts to address "alleged heightened risk of technologies being used by adversaries for military ends."[125] Yet that does not seem to have been the focus of the DTC Amendment Act—indeed, reliance upon the DSGL has not wavered.

That creates several issues for AUKUS research in Australian HEIs. Firstly, the exercise of the President's power to proscribe defense articles and defense services is an exercise of executive power, not legislative. The ITAR specifically denies judicial review,[126] and appeals for decisions under the EAR are extremely limited.[127] Both the EAR and ITAR are also exempted from the usual operation of US judicial review legislation,[128] and the Supreme Court has recently taken the view that allowing appeals against the President's executive power risks 'structural spillover'.[129] By comparison, the DSGL is a legislative instrument made by the Minister for Defence.[130] It is potentially subject to disallowance by Parliament,[131] and grounds for judicial scrutiny of the legality of DTCA decisions are also

---

[121] Thom, *Independent Review,* p. 29.
[122] Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* pp. 17-18.
[123] Tesch, Samuel, *Independent Review,* pp. 6 and 11-12.
[124] Sanders, "Australia's defense export control regime and critical technologies," p. 11.
[125] Sanders, "Australia's defense export control regime and critical technologies," p. 13.
[126] 22 U.S. Code § 2778(h).
[127] 15 CFR §§ 756.2 and 756.3.
[128] 5 U.S. Code §§ 701-706; see also *Karn v United States Department of State*, 925 F. Supp. 1 (D.D.C. 1996), where a claim that export control laws were in violation of the First and Fifth Amendments of the *US Constitution* was held to be non-justiciable.
[129] That is, the 'danger that a judicial decision against the Executive or Congress could impair the effective performance of the political branches in the roles that the Framers [of the US Constitution] envisioned': Peter Margulies, 'The Travel Ban Decision, Administrative Law, and Judicial Method: Taking Statutory Context Seriously' (2019) 33 *Georgetown Immigration Law Journal* 159, 161.
[130] Sections 112(2A)(aa) and (2AA).
[131] Particularly section 42.

available.[132] Availability of judicial remedies are a welcome difference between the Australian and US systems,[133] but the possibility remains that matters of high policy should not be permitted to be tied to political or private economic interests, rather than those of the national security and foreign policy of the nation.

Secondly, there is a mismatch in regulatory scope with the DSGL. Export controls are usually focused on military and dual-use technologies, whilst research security takes a broader view of examining and securing technologies that might be classed as 'in the national interest' (including for reasons of national or economic security, or foreign policy reasons).[134] Numerous of these technologies concurrently form part of the research appetite at HEIs, an interest that will only increase when AUKUS starts to contribute funding opportunities to research. Yet the definition of 'DSGL technology' in the DTCA, and the offences to which that definition relates,[135] will still refer solely both military (Part 1) and dual-use (Part 2) technologies. In the US, this regulatory mismatch between military technology and technology 'in the national interest' is found in the EAR, a system which Australia has not adopted. Put another way, Australia has fundamentally transformed its export control laws to contain provisions comparable to the ITAR, but without creating a less onerous framework analogous to the EAR for dealing with those technologies 'in the national interest'.[136] In other words, Australia still lacks a cohesive system that allows for the proscription (and therefore protection) of technologies which ought to be protected on economic, foreign policy, or national security grounds. This has obvious implications for research security

[132] DTCA, s 63(1); *Re Bolton, Ex parte Bean* (1987) 162 CLR 514; *Coco v R* (1994) 179 CLR 427; cf. *Thomas v Mowbray* (2007) 233 CLR 307 where the High Court of Australia considered the separation of the powers doctrine.

[133] Noting that there have been no Parliamentary or judicial challenges of the DSGL to date.

[134] In the US these are referred to as 'Critical and Emerging Technologies' whilst in Australia they are 'Critical Technologies in the National Interest': "Critical and Emerging Technologies List Update," National Science and Technology Council, accessed 17 September 2024; cf. "List of Critical Technologies in the National Interest," Department of Industry, Science and Resources, May 2023.

[135] DTCA, ss 10-10C.

[136] In evidence to the Senate Committee, the Australian Strategic Policy Institute explained it this way: '[s]ubstantial efforts at reform in the US have focused on moving goods and services requiring lower levels of scrutiny from ITAR to EAR and loosening the latter set of rules to align more closely with national security requirements': Senate Committee (n 94) 17.

because technologies 'in the national interest' risk being underregulated or not regulated at all.[137]

Thirdly, emerging technologies can be difficult to capture with export control frameworks, both at international and domestic levels.[138] In the US, this was dealt in part through the Export Control Reform Act of 2018, which permits the Department of Commerce (the same regulatory agency for the EAR) to publish new rules which link 'emerging technologies' not only to forms of export control through the EAR, but also limit foreign direct investment in their development under the Foreign Investment Risk Review Modernization Act of 2018 (such investment also can come under the scrutiny of the Committee on Foreign Investment in the United States (CFIUS)).[139] Australia has no such link between its DTCA and mechanisms for either foreign investment,[140] nor its policy vehicles for examining critical technology investment.[141] Instead, Australian HEIs will likely end up carrying the risks of conducting research (and managing the investment) into these emerging technologies until such time as the government realizes there might be a security problem. That is itself a huge threat, given the government in Australia has a poor history of realizing security problems in emerging tech, evidenced by media findings that foreign-made drones were in active use by the Australian Defence Force[142] and foreign-made cameras were installed in Parliament House.[143]

End-use and retransfer control commitments

A significant difference between the DTCA and US export control laws is the lack in the former of end-user specific regulations; that is, controls

---

[137] Go Yoshizawa, et al., "Limiting open science? Three approaches to bottom-up governance of dual-use research of concern," *Pathogens and Global Health,* 4 (2024), p. 285.

[138] International Panel on the Regulation of Autonomous Weapons (iPRAW), *LAWS and Export Control Regimes: Fit for Purpose?* (Report, 2020).

[139] Scott A. Jones, "Trading Emerging Technologies: Export Controls Meet Reality," *Security and Human Rights*, (2021), pp. 5-7.

[140] Under the Foreign Acquisitions and Takeovers Act 1975 (Cth); cf. the moves by the UK to limit investments in such technologies under the National Security and Investment Act 2021 (UK).

[141] Such as the Department of Industry's List of Critical Technologies in the National Interest (website, May 19, 2023) <https://www.industry.gov.au/publications/list-critical-technologies-national-interest>.

[142] Ellen Whinnett, "Defence chiefs order grounding of China's DJI drones pending six-month security audit," *The Australian*, May 5, 2023.

[143] 9News, Minister orders removal of China-linked cameras from defence premises, *9News*, February 9, 2023.

intended to keep the arms in the hands of the original recipient whilst also verifying that recipients use such articles 'only for permitted purposes'.[144] Notionally, end-user monitoring is an international obligations of the ATT, acting to prevent diversion and black market sales.[145] Both the ITAR and EAR are intended to operate extraterritorially to constrain the US from exporting technologies and data in circumstances where it cannot be satisfied that the security of those technologies and data will be preserved.[146]

An extremely powerful provision of research security could have come from Australia adopting the End-User and Entity Lists of the EAR (again, by recalling that the power of export control is the flexibility of lists to "control who may research"). Those provisions permit the President to publish a list of "foreign persons and end-uses that are determined to be a threat to the national security and foreign policy of the United States."[147] Further, the AECA stipulates that the President may determine that a country has "engaged in a consistent pattern of acts of intimidation or harassment directed against individuals in the United States", the practical consequence of such a finding being that "[n]o letters of offer may be issued, no credits or guarantees may be extended, and no export licenses may be issued…"[148]

Australia has no similar scheme in place to prohibit dealings with named foreign entities, relying solely on trust that HEIs are checking any relevant sanctions or end-user lists proactively. The DTCA also has no such provisions, and there appears no Parliamentary intention for Australia to so closely link its foreign policy agenda to its export control framework. Indeed, it seems Parliament intended to keep the DTCA as a "permissive" statute.[149] The Minister may publish a list of foreign countries to whom exchanges will not be covered by the offence provisions in the DTCA, they may not do so unless they are satisfied that "specifying the foreign country in the instrument is in the interests of Australia's national security,

---

[144] 22 U.S. Code §§ 2778(g)(7) and 2785(a).

[145] Even if the prevalence of predominantly US-manufactured weapons in conflict zones around the world might challenge that assertion: Jennifer L. Erickson, "Saint or sinner? Human rights and US support for the arms trade treaty," *Political Science Quarterly,* 130(3) (2015), p. 449; Trevor Thrall, Caroline Dorminey, *Risky business: the role of arms sales in U.S. foreign policy* (Policy Analysis No. 836, CATO Institute); Jennifer L. Erickson, "Demystifying the 'gold standard' of arms export controls: US arms exports to conflict zones," *Global Policy,* 14 (2023), p. 131.

[146] 22 CFR §§ 127.1(c), 123.9(b) and (c), 123.10(a) and 124.8(5).

[147] 50 U.S. Code §§ 4812(b)(1), (5) and (7).

[148] 22 U.S. Code §2756.

[149] Revised Explanatory Memorandum to the Defence Trade Controls Amendment Bill 2023, p. 3.

Australia's foreign relations or Australia's national economic well-being."[150] The wording of that section does not however permit the Minister for Defence to use export control laws to prevent exchanges with countries or entities for whom it is not in Australia's interests.[151]

Another issue is the DTCA's handling of intangibles. For example, the ITAR prohibits the export of 'defense services'—the technical knowledge or capability enabling or supporting the use of particular technologies—in the same manner as both defense articles and technical data.[152] A similar provision in the EAR provides that exports of technologies are very broadly defined, such that the EAR describes the "release of technology to a foreign national in the United States through such means as demonstration or oral briefing is deemed an export."[153] Thus, providing intangibles to a foreign person is *prima facie* unlawful, depending only on where the release or transfer occurred.[154] It appears this was the basis that Daniel Duggan, a former US Air Force pilot accused of training Chinese pilots on how to land safely on aircraft carriers at sea, is now facing extradition from Australia to face charges related to breaching the ITAR.[155] For serving members and civilians in Australia's Defence Force and Department of Defence, amendments to the Defence Act 1903 (Cth) by the Defence Amendment (Safeguarding Australia's Military Secrets) Act 2024 (Cth) have also now created an obligation to seek a Ministerial "foreign work authorisation" if they wish to "work for, or providing training to, a foreign military or government body".[156]

Although the DTCA reforms do go some way to prohibiting the transfer of intangible forms of technology (such as the "deemed export" offences of section 10A and the provision of a "defense services" offence of section 10C), there is still plenty of room for research security concerns to manifest. For example, an international student attending a HEI may conduct research on DSGL technology as part of a research initiative

---

[150] DTCA, s 15(4AA); see also the Defence Trade Controls Act 2012 - Foreign Country List (Cth).

[151] Although Australian law does provide some power to do so, that power is reposed in the Foreign Minister, and may only be exercised if an arrangement 'adversely affects, or is likely to adversely affect, Australia's foreign relations; or…is, or is likely to be, inconsistent with Australia's foreign policy': Australia's Foreign Relations (State and Territory Arrangements) Act 2020 (Cth), ss 35(1), 36(1) and 40(1).

[152] 22 CFR §§ 120.2, 120.3(a)(1) and 120.10.

[153] 15 CFR §730.5(c).

[154] 22 CFR §§120.50(a)(2) and 120.51(a)(2).

[155] Clareese Packer, Adelaide Lang, "Daniel Duggan case: "Mr Duggan is eligible for surrender" over Chinese fighter pilots training claims", *The Australian*, May 24, 2024.

[156] "Safeguarding Australia's Military Secrets", Department of Defence, accessed 19 September 2024, <https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/safeguarding-australias-military-secrets>.

between the HEI and the Department of Defence, then carry that knowledge with them back to their host country and supply it to their government.[157] Depending on the circumstances, this might not be a supply of DSGL technology "from in Australia to outside Australia" (section 10), "in Australia to a foreign person" (section 10A), "supply from outside Australia" (section 10B), nor a provision of DSGL services (section 10C), because it is not a 'constitutional DSGL service' nor a 'relevant DSGL service'.[158]

What seems strangest of all is that despite both the statutory reviews of the DTCA recommending investigation and enforcement powers to promote compliance with the DTCA,[159] the DTC Amendment Act did not provide them, and there appears little political appetite to do so.[160] Such powers could have (albeit indirectly) provided for uplifted research security across Australian HEIs, by ensuring a strong culture of compliance with both the DTCA provisions re-export obligations incurred receiving defense articles, technical data and defense services. In that absence, it remains entirely unclear on publicly available information whether Defence Export Controls (DEC)—the body in the Department of Defence responsible for such compliance activities—undertakes any compliance activities or has ever prosecuted any person for breaches of Australian export control laws.[161]

Part V: Possible solutions

Having missed the opportunity to reform export controls in a manner that would have been conducive to research security, the door has not completely shut for the Australian government. However, I believe it is unlikely (barring any catastrophic event or monumental change in government) that the DTCA will be amended so shortly after the DTC

---

[157] The precise parameters of migration controls over students are not within the scope of this paper. For a more fulsome examination, see Brendan Walker-Munro, "Risks of Espionage in our Universities? What Lessons on Research Security Can Australia Learn from the case of *Li v Canada*," *Adelaide Law Review*, forthcoming(2025).

[158] DTCA, ss 5B(2) and 5C(2).

[159] Thom, *Independent Review,* pp. 45-46; Tesch, Samuel *Independent Review,* p. 9.

[160] Stating that "Defence will work with the Australian Federal Police, industry, academic and research sectors… to determine the most appropriate mechanism to fulfil this function"; "Government Response to the Defence Trade Controls Act Review," Department of Defence, accessed 20 September 2024) https://www.defence.gov.au/about/reviews-inquiries/independent-review-defence-trade-controls-act-2012.

[161] "Our Performance," Defence Export Controls, March 2023, <https://www.defence.gov.au/business-industry/export/controls/about/performance>.

Amendment Act. The policy objective of that amendment was achieved; that is, to bring Australian export controls into rough 'comparability' with the US ITAR to facilitate the onward progress of AUKUS. The unintended consequences of the government's shortsightedness will likely make themselves known over the coming years—whether this results in the maligned 'standardized' approaches to risk said to endangers the plurality of voices intended to be heard on matters of academic publication, open science, freedoms of expression and creative thought remains to be seen.[162] At the same time, academics have every right to be disappointed by their ongoing securitization. Similar types of amendments made to EU dual-use controls since 2000 have largely "shift[ed] the attention of regulatory oversight to the stage of science and technology development and makes researchers effectively co-responsible for the politics of security."[163]

What then could be done to rectify this situation? No amount of arguing *ex post* is likely to shift an export control regime that has resisted the recommendations of two separate statutory reviews. Instead, academia and industry will need to work more closely with government within the parameters that Parliament has set in the DTCA and relying more fulsomely on non-law solutions such as policy, collaborative endeavors (such as boards and combines) and as much alignment of language around export control as possible. Given that many global jurisdictions are still settling the definitional arguments about what 'research security' encompasses (or even what to call it), these same non-law programs are the ones suggested in emerging research security literature.[164] Therefore, I submit that by taking these simple measures, our HEIs might be in a better position to protect the jewels of the AUKUS crown from theft or dissemination.

---

[162] Dagmar Rychnovská, "Security meets science governance: The EU politics of dual-use research", *Emerging Security Technologies and EU Governance,* ed. Antonio Calcara, Raluca Csernatoni and Chantal Lavallee (Routledge, 2020), pp. 164-176.

[163] Rychnovská, "Security meets science governance", pp. 164-176.

[164] For example, see the work of Tommy Shih, who argues for an increased role for research funding bodies: Tommy Shih, "The role of research funders;" as well as individual awareness and collaborative practice at a global level: Tommy Shih, "Points of departure and developing good practices for responsible internationalization in a rapidly changing world," 31(2) (2024), *Accountability in Research,* p. 1; Tommy Shih, "Recalibrated responses needed to a global research landscape in flux," *Accountability in Research,* 31(2) (2024), p. 73.

The role of adjudicative bodies

Acting outside of the formalized legal structures of their host States, there has been an increase in the use of adjudicative bodies (or advisory bodies with quasi-adjudicative power) to settle disputes or provide interpretative guidance in a number of regimes that are co-regulatory to export control. In some respects, these bodies operate like their international export control counterparts like the Wassenaar Arrangement and the Australia Group, by providing broad guidelines around what technologies States should be regulating and the mechanisms for that regulation.[165]

In the life sciences for example, the boundaries between research that is safe to both researchers and institutions, and that which poses a grave threat to biological security and public health, can be razor thin. The conduct of 'dual use research of concern'—generally speaking, the provision of pathogens with characteristics or functions which they do not naturally possess and may pose public health risks[166]—has seen the formulation of at least two bodies, the National Science Advisory Board for Biosecurity (NSABB) in the US[167] and the Israeli Council for the Regulation of Research with Disease Pathogens.[168] In both cases, these bodies have been established to straddle the divide between concerns over national security and academic freedom, to shoulder the burden of both worlds, such that they act by:

> "…building on the bona fides of their distinguished members, their legitimacy emanates from their commitment to include competing perspectives. These new mechanisms may thus be more apt to handle the blurring science-state boundaries…Enforcing strict boundaries may even be counterproductive, and it may be necessary to emphasize a diplomatic approach over bureaucratic solutions, mediation over demarcation, inclusive deliberation over neutral competence."[169]

---

[165] Michael D. Beck, Scott A. Jones, "The once and future multilateral export control regimes: innovate or die," *Strategic Trade Review,* 5(8) (2019), p. 55.
[166] National Academies of Sciences, Engineering, and Medicine, *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies* (National Academies Press (US), Washington DC, 14 September 2017).
[167] Evans, Valdivia, "Export controls and the tensions between academic freedom and national security," p. 186.
[168] Ori Lev, "Regulating dual-use research: Lessons from Israel and the United States," *Journal of Biosafety and Biosecurity,* 1(2) (2019), p. 80.
[169] Evans, Valdivia "Export controls and the tensions between academic freedom and national security," p. 186; see also Wilner et al., "Research at risk," p. 48.

Both the NSABB and the Israeli Council may issue recommendations or advisory opinions about the application of export controls to research in the life sciences which could pose a national security risk. Though such recommendations are not of themselves binding, given that the ITAR permits restrictions not just in the interests of 'national security' but also 'for proprietary or national security reasons',[170] it is at least arguable that certain publications subject to an NSABB recommendation could be excluded from the FRE and an export license required to support publication or disclosure.[171] Japan has operated a similar body—the Center for Information on Security Trade Control—since the 1990s with resounding success.[172]

Australia has no such adjudicative or guidance-setting bodies under the provisions of its export control framework but could clearly benefit from one: the Thom Review, Senate Committee and Tesch/Samuel Review all heard from members at the defense-industry and defense-academia interface complaining of issues in interpretation, consistency, and guidance on the content of both the DTCA and DSGL.[173] Such a board or body should not be merely limited to the life sciences, but could be comprised of representatives from academia, defense industry, as well as the departments of Defense, Foreign Affairs, Home Affairs and the intelligence community. That body could then consider submissions about potential dual-use technologies of potential concern on a voluntary (even anonymous) basis, either from researchers across Australia's HEIs and the intelligence community. The decisions of such a body would not be legally binding, but would be useful voices of guidance, especially for researchers who appear to bear the brunt of ensuring compliance under the revised DTCA.

The NSABB has been criticized in the past based on its membership and mandates, with some suggesting that the predominance of influenza experts has improperly influenced their biosafety and biosecurity policy

---

[170] 22 CFR §§120.34(a)(8) and 120.43.

[171] Christos Charatsis, "Setting the publication of "dual-use research" under the export authorisation process: "the H5N1 case," *Strategic Trade Review,* 1(1) (2015), p. 56.

[172] Bates Gill, Kensuke Ebata, Matthew Stephenson, "Japan's export control initiatives: Meeting new nonproliferation challenges," *The Nonproliferation Review,* 4(1) (1996), pp. 30, 36-37; CISTEC, "The Center for Information on Security Trade Controls (CISTEC) Export Control Model of Japan: Role, Utility, and Management," *Strategic Trade Review,* 5(8) (2019), p. 77.

[173] Thom, *Independent Review*, p. 23; Senate Standing Committee, *Defence Trade Controls Amendment Bill 2023,* pp. 17-18; Tesch, Samuel, *Independent Review,* pp. 6 and 11-12.

decisions, especially in the wake of COVID-19.[174] The establishment of an advisory body for export control would equally be marred at commencement by the same arguments around offering everyone a seat at the table whilst simultaneously deciding whose voices should be heard and whose should not. Empirical evidence in the export control sector is rare, but what does exists suggests that States which adopt new export control laws then "tend to get bogged down in the institutionalization and implementation phases of export control development."[175] That said, one of the more interesting recommendations of the Tesch/Samuel Review involved Defence developing "an accreditation system to build and maintain a cadre of export control compliance advisors"[176] to provide advice to HEIs on their export control obligations, so perhaps the notion of an advisory body on export controls in Australia is not as improbable as it seems.

Deepening relationships between government, industry and academia

Another avenue for Australia to resolve shortcomings in the export control system could involve better integration and coordination of export controls within and between those who administer the scheme (i.e., DEC and Defence) and those subject to it (HEIs). This could encompass anything from information-sharing networks to truly co-designed complexes or clearinghouses. According to the emerging literature on these forms of informal governance, these "trusted communities" require the inclusion of three classes of stakeholders to be successful:[177]

- State actors, who have an understanding of the policy reasons for export control but usually lack the necessary technological know-how of emerging or dual-use technologies;

---

[174] National Academies of Sciences, Engineering, and Medicine, *Dual Use Research of Concern,* p. 42; Dana Perkins, Lela Bakanidze. "Examples of Biorisk Management National Regulatory Frameworks", *Essentials of Biological Security: A Global Perspective*, ed. Lijun Shang, Weiwen Zhang and Malcolm Dando, (Wiley, online, 2024), pp. 173-187.

[175] Douglas M. Stinnett, et al., "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives,* 12 (2011), pp. 308, 323.

[176] Tesch, Samuel, *Independent Review*, p. 7.

[177] Brigitte Dekker, Maaike Okano-Heijmans, "Emerging Technologies and Competition in the Fourth Industrial Revolution: The Need for New Approaches to Export Control," *Strategic Trade Review,* 6(9) (2020), p. 53; Machiko Kanetake, "Dual-Use Export Control: Security and Human Rights Challenges to Multilateralism", *European Yearbook of International Economic Law,* ed. Marc Bungenberg, et al. (Springer International, Cham, 2020), pp. 265-290.

- Researchers and HEI representatives, who possess a narrow but deep area of expertise relevant to the more difficult interpretations of export control applications; and
- Industry participants, who have a fundamental understanding of economic applications of technologies but are generally financially motivated to search for self-imposed or voluntary regulatory standards to prevent lawmaking (which may be more obligatory or stifling).

These forms of trusted communities require a more fulsome level of disclosure by State actors than is usually the case with forms of government stakeholder engagement, i.e., roundtables, consultation groups etc., but the benefits can be incredibly worthwhile. These groups can deliver strong benefits, including broader legitimacy flowing from their inclusiveness and range of expertise to a more coherent setting of policy deriving from unified views on policy.[178] Such relationships can also help smaller industry players get their foot in the door with government, promote best-practice and information distribution, as well as providing a vehicle for government to "sensitize enterprises operating in the field to a variety of evolving export control concerns."[179]

Such communities are already in existence, including in Australia, in other fields. For example, the FINTEL Alliance operates in the field of anti-money laundering as an intelligence and innovation clearinghouse between banks and the financial intelligence regulator AUSTRAC.[180] The Alliance co-opts staff of banks as secondees to AUSTRAC, subjecting them to security clearances but then allowing them access to AUSTRAC's significant intelligence holdings. Not only can this allow true cooperation in terms of operational matters (by allowing the rapid dissemination of accurate information through webs of trusted influence across the banking sector), but the Alliance also incorporate an "Innovation Hub", where potential new challenges to the system can be sandboxed and a variety of perspectives gained to inform government policymaking.

Even more recently, the National Science Foundation in the US has announced $67 million in funding to create the SECURE Centre, a collaborative initiative allowing information-sharing across business,

---

[178] Dekker and Okano-Heijmans, "Emerging Technologies and Competition," pp. 65-66.
[179] Dekker and Okano-Heijmans, "Emerging Technologies and Competition," pp. 65-66.
[180] Paula Chaddington, Simon Norton, *Public-Private Partnerships to Disrupt Financial Crime: An Exploratory Study of Autsralia's FINTEL Alliance* (SWIFT Institute Working Paper NO. 2017-003, May 28, 2019).

government and academia.[181] Led through the University of Washington and Texas A&M, it is intended the Centre will ""will link members of the U.S. research community from institutes of higher learning, nonprofits and businesses in a safe, trustworthy platform to share ideas, needs and information on research security."[182] Such a "trusted community" could very easily be established in Australia to help bridge the gap between government and academic expectations in relation to export controls and research security.

Improving other research security protections

The final option open to Australia is to improve the interaction of export controls with other mechanisms of research security in Australian HEIs. There are many opportunities for improvement, especially in Australia which lacks a cohesive governmental policy on research security in the same vein as its AUKUS partners.

Perhaps then, that is the first step—a comprehensive Commonwealth policy on research security. After all, the US already has both comprehensive policies formulated by the National Science Foundation, supported by several Presidential proclamations including the National Security Presidential Memorandum No 33[183]—and directives from the President's Office of Science and Technology Policy.[184] The National Institute for Science and Technology published the Safeguarding International Science: Research Security Framework in 2023,[185] specifically designed to provide uniform implementation guidance for HEIs.

The Australian government's efforts—typified in the UFIT Guidelines[186]—are not only in need of significant refreshment, but also a system of implementation guidance and monitoring that ensures Australian HEIs

---

[181] National Science Foundation, NSF-backed SECURE Center will support research security, international collaboration (Media release, July 24, 2024) <https://new.nsf.gov/news/nsf-backed-secure-center-will-support-research>.

[182] National Science Foundation, NSF-backed SECURE Center.

[183] Office of the US President, NSPM-33 Presidential Memorandum.

[184] Eric Lander, *Clear Rules for Research Security and Researcher Responsibility* (Office of the US President, 10 August 2021); Arati Prabhakar, *Guidelines for Research Security Programs at Covered Institutions* (Office of the US President, 9 July 2024).

[185] Gregory F. Strouse, Claire M. Saundry, Timothy Wood, Philip Bennett, Mary Bedner, *Safeguarding International Science: Research Security Framework* (NIST, August 31, 2023).

[186] *Guidelines to counter foreign interference in the University Sector,* Department of Education.

have adopted the protections they call for. This in turn will require a far more significant acknowledgement of research security policy, and the role played by export controls in Australian HEIs, than has ever been the case. The government may very well need to 'put its money where its mouth is', especially in an environment where universities are being squeezed for international student income.[187]

At the far end of the scale, the Australian government may need to consider other forms of legislation to buttress the weaknesses in the export control system. For example, this may require the incentivization of using patents or other forms of intellectual property protection to ensure that novel developments in HEIs cannot be spirited away by foreign actors (or at least creates stronger disincentives for them to do so).[188] Alternately, Defence could start to make its efforts on enforcing export controls more visible—assuming they are performing them at all. The high visibility of the Export Control Joint Unit (ECJU) in the UK could be a good starting point. ECJU routinely publishes new and updated guidance specifically for HEIs, as well as case studies and three-monthly statistics on all audits and activities performed under UK export control law.[189]

Part VIII: Conclusion

The role of Australia's export controls is to tread a fine line between allowing the innovations and collaborations which drive multidisciplinary and open research to flourish, whilst protecting potentially sensitive technologies or those with a military end-use from diversion to States contrary to our national interests. In that context, Australia's DTCA plays an incredibly important supporting role in ensuring the cutting-edge research conducted at our HEIs is performed safely, securely, and without the grave risk of foreign interference or malign influence.

The passing of the DTC Amendment Act should also have been a watershed moment in Australian research security, a time where government listened to both industry and academia to enact a set of controls that would prepare Australian researchers for participation in a

[187] See for example submissions to the current controversy involving overseas student caps: Senate Standing Committee on Education and Employment, *Education Services for Overseas Students Amendment (Quality and Integrity) Bill 2024 [Provisions]* (July 2024).
[188] Aineas Kostas Mallios, "Licensing and secrecy under imperfect intellectual property protection," *Theory and Decision*, (2024).
[189] "Export Controls," Export Control Joint Unit, accessed 10 October 2024, <https://www.gov.uk/government/organisations/export-control-joint-unit >.

highly contested geopolitical environment. Instead, the recommendations of two statutory reviews have been supplanted by political necessity, with only the barest amendments needed to ensure bottom-line comparability with the US ITAR and EAR to support the progression of the AUKUS Agreement.

Time will tell what such political expediency has really paid for in terms of the research security of our HEIs. This paper has sought to explore some potential policy options to fix shortcomings in Australian export control law, but what is really needed is a more ambitious legislative agenda that treats research security as a genuine topic of discussion. That in turn requires academic debate and critique, not only of governmental actions taken to advance research security, but the discipline itself. In doing so, the government must also be willing to accept where it has not met the mark, especially in comparison to our international partners. Anything less will see Australia potentially taking up the mantle as the 'weak link' in the AUKUS chain.