(PROFESSOR) HADRIAN'S WALL: THE ROLE OF THE AUSTRALIAN RESEARCH COUNCIL IN SECURING UNIVERSITY RESEARCH

BRENDAN WALKER-MUNRO*

Research security is the action of protecting sensitive, classified or commercially valuable knowledge and technologies from espionage, theft, interference and illicit transfers. Yet academic explorations of research security are still at their most formative stages. This is especially the case in Australia and its universities, which has been accused in recent years of falling behind research security efforts compared to other Western nations such as the United States ('US'), Canada, the United Kingdom and the European Union ('EU'). This article has two purposes. The first is to highlight the important role that the Australian Research Council ('ARC') has played in providing Australian research security. The second purpose of this paper is to illustrate the significant undeveloped potential for the ARC. Drawing on examples from the funding bodies in the US and Canada (including recent changes to their enabling statutes and regulations), this article argues for an increased role for the ARC in securing the university research enterprise.

I INTRODUCTION

Australia currently faces its most significant intelligence and national security environment since the Cold War. The country is currently set between the geopolitically ambitious reach of China – which has been accused of mounting and maintaining an industrial scale network to steal intellectual property,[1] among other actions of foreign policy – and the increasingly fraught negotiations of the AUKUS Agreement.[2] Indeed, the apparent battle is at such a fever pitch that it led Mike

* Senior Lecturer, Southern Cross University.

1 Jade Macmillan and Andrew Greene, 'ASIO Director Tells Five Eyes Intelligence Summit That Alleged Chinese Spy Was Removed from Australia', *ABC News* (online, 18 October 2023) <https://www.abc.net.au/news/2023-10-18/five-eyes-spy-summit-asio-cia-fbi-san-francisco/102984976>.

2 Andrew Greene, 'Pentagon Sparks Fresh AUKUS Doubts on Anniversary of Australia's Nuclear-Powered Submarine Plans', *ABC News* (online, 13 March 2024) <https://www.abc.net.au/news/2024-03-13/us-defence-announcement-raises-questions-on-aukus-anniversary/103578408>; Ben Westcott, 'Australia Faces Aukus Nuclear Submarine Concerns as US Order Cut', *Bloomberg* (online, 13 March 2024) <https://www.bloomberg.com/news/articles/2024-03-13/australia-faces-aukus-nuclear-submarine-

Burgess, Director-General of the Australian Security Intelligence Organisation ('ASIO'), to remark last year that it felt like his officers were engaged in 'hand-to-hand combat' with our adversaries.[3]

In that context, universities face a unique and rising challenge. Previously funded by incredibly high engagement with international student cohorts and research arrangements with international entities,[4] institutions of higher education are now being forced to question the closeness of these associations. In the contemporary spotlight, Chinese universities and academics are enrolled in 'civil-military' fusion programs, where ostensibly civilian institutions are given access to classified information in exchange for hosting military officers or security service executives as faculty members.[5] Independent reporting has also suggested that universities have been specifically named as targets by foreign intelligence services,[6] as well as detailing a litany of data breaches, leaks and active intelligence gathering occurring on campuses around the world.[7]

Though countries like Russia, China and Iran top the lists of most concerning state actors, there are also actions being attributed to nations previously aligned (or at least not opposed) to Western interests. In late 2023, reports emerged of a Malaysian student being arrested in Norway on espionage charges after allegedly eavesdropping on the office of the Prime Minister and Defence Ministry.[8] Three months later (again in Norway) a Brazilian university professor was arrested for espionage, and subsequently alluded to being a member of Russian military

---

concerns-as-us-order-cut>; Matthew Cranston and Andrew Tillet, 'Albanese, Pentagon Looks to Allay AUKUS Submarine Fears', *Australian Financial Review* (online, 13 March 2024) <https://www.afr.com/world/north-america/pentagon-looks-to-allay-aukus-submarine-fears-20240313-p5fbye>.

3 Mike Burgess, 'Director-General's Annual Threat Assessment', *Australian Security Intelligence Organisation* (Transcript, 21 February 2023) <https://www.asio.gov.au/director-generals-annual-threat-assessment-2023>.

4 For the risk of these arrangements, see Brendan Walker-Munro, David Mount and Ruby Ioannou, *Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education* (Report, 30 October 2023). See also Radomir Tylecote and Robert Clark, *Inadvertently Arming China? The Chinese Military Complex and Its Potential Exploitation of Scientific Research at UK Universities* (Report, Civitas, 24 February 2021).

5 Alex Joske, *The China Defence Universities Tracker* (Report, Australian Strategic Policy Institute, 25 November 2019) <https://www.aspi.org.au/report/china-defence-universities-tracker> ('*China Defence Universities Tracker*').

6 Ana Swanson and Keith Bradsher, 'White House Considers Restricting Chinese Researchers Over Espionage Fears', *The New York Times* (online, 30 April 2018) <https://www.nytimes.com/2018/04/30/us/politics/trump-china-researchers-espionage.html>.

7 The National, 'Iranian Hackers Behind Stolen Research from British Universities', *The National* (online, 15 September 2018) <https://www.thenationalnews.com/world/europe/iranian-hackers-behind-stolen-research-from-british-universities-1.770313>; Amy Qin, 'As US Hunts for Chinese Spies, University Scientists Warn of Backlash', *The New York Times* (online, 28 November 2021) <https://www.nytimes.com/2021/11/28/world/asia/china-university-spies.html>; Ken Dilanian, 'American Universities Are a Soft Target for China's Spies, Say US Intelligence Officials', *NBC News* (online, 3 February 2020) <https://www.nbcnews.com/news/china/american-universities-are-soft-target-china-s-spies-say-u-n1104291>; Gordon Corera, 'Iranian Hackers Posed as British-based Academic', *BBC News* (online, 13 July 2021) <https://www.bbc.com/news/technology-57817463>.

8 Munira Mustaffa, 'No Neutrality in Espionage: Why Is Malaysia Tangled Up in a Spying Case in Norway?', *The Interpreter* (online, 19 September 2023) <https://www.lowyinstitute.org/the-interpreter/no-neutrality-espionage-why-malaysia-tangled-spying-case-norway>.

intelligence.[9] And Saudi Arabia – a country certainly no stranger to scandals – has been linked to efforts for more than a decade to lift its academic profile by 'buying' publication affiliations in research journals.[10]

Internationally, universities have enacted programs of 'research security' to protect vulnerable research and researchers from foreign interference, espionage and intellectual property theft. These programs take a variety of approaches, from education on the issues, risk management for both research and researchers, and application of specific legal restrictions such as immigration and export controls.[11] A key element in contemporary research security has been a focus on cybersecurity, where universities have long struggled to protect themselves.[12] Harvard University in the United States ('US') has enacted specific data management obligations on all staff,[13] whilst in Canada the U15 (representing the most research-intensive universities) has published guidance on inter alia institutional data management and data security.[14]

Australian universities are no less vulnerable to these forms of physical and digital infiltration, coercion and manipulation. In 2022, a report released by the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') on national security risks at Australian universities expressed their concern 'that incidents of foreign interference, censorship and intimidation were occurring on university campuses'.[15] The PJCIS also reflected on the roles of universities in that inquiry ('PJCIS Inquiry'), saying further that:

> …[t]he sector has not, and did not, respond to these risks in a vacuum or of their own proactive volition. Because of this reactionary approach, the Committee took a dim view of arguments of legislative overlay and increasing regulatory burdens

---

9 Ty Roush, 'Man Accused of Being Spy Admits He's Russian after Years Posing as Academic in Norway, Canada', *Forbes* (online, 14 December 2023) <https://www.forbes.com/sites/tylerroush/2023/12/14/man-accused-of-being-spy-admits-hes-russian-after-years-posing-as-academic-in-norway-canada>.

10 Yudhijit Bhattacharjee, 'Saudi Universities Offer Cash in Exchange for Academic Prestige' (2011) 334(6061) *Science* 1344, 1344–5 <https://doi.org/10.1126/science.334.6061.1344>; SIRIS Academic, *The Affiliation Game of Saudi Arabian Higher Education and Research Institutions* (Report, 3 May 2023) 16–23.

11 'Science and Security', *Association of American Universities* (Web Page, 2024) <https://www.aau.edu/key-issues/science-security>.

12 Ivano Bongiovanni, 'The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education' (2019) 86 *Computers and Security* 350 <https://doi.org/10.1016/j.cose.2019.07.003>; Peter Romness, 'Securing University Research: An Industry Perspective', *Cisco Blogs* (Blog Post, 13 April 2021) <https://blogs.cisco.com/education/securing-university-research-an-industry-perspective>; Jin Li, Wei Xiao and Chong Zhang, 'Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents' (2023) 10 *Humanities and Social Sciences Communications* 270:1–18 <https://doi.org/10.1057/s41599-023-01757-0>.

13 'Research Data Security and Safety', *Research Support at Harvard* (Web Page) <https://researchsupport.harvard.edu/research-data-security-and-safety>.

14 Government of Canada, *Safeguarding Research in Canada: A Guide for University Policies and Practices* (Web Page, 22 June 2023) <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-research-organizations-funders-and-universities/safeguarding-research-canada-guide-university-policies-and-practices>.

15 Parliamentary Joint Committee on Intelligence and Security, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (Report, March 2022) 117 [6.13] <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024611/toc_pdf/InquiryintonationalsecurityrisksaffectingtheAustralianhighereducationandresearchsector.pdf> ('*PJCIS Report*').

> when the Committee considers that the sector was being reactionary to the national security risks. It is possible perhaps that should the sector have been more proactive on issues like talent recruitment and foreign interference on campuses that additional government intervention would not have occurred.[16]

During that same inquiry by the PJCIS, the role of the Australian Research Council ('ARC') was examined. Alongside the Commonwealth Scientific and Industrial Research Organisation ('CSIRO') and National Health and Medical Research Council ('NHMRC'), the ARC is a significant supplier of investment in Australian university research. During the inquiry, the ARC highlighted the incredible contribution of Australian research – producing 'approximately 3 per cent of global scientific output while being home to only 0.34 per cent of the global population'.[17]

The ARC also agreed that espionage and foreign interference posed a significant risk to university endeavours. Their evidence to the PJCIS agreed that 'it is critical that the work of Australian researchers is not compromised by foreign interference that may put universities' people, information, intellectual property and data, or national security at risk'.[18] At the same time, the PJCIS also heard evidence that two Australian professors, George Zhao and Xue Jingling, allegedly received funding from the ARC whilst supplying access and details on the funded technology to partners in China (including partners with links to the People's Liberation Army).[19]

This article therefore seeks to explore the role played by the ARC in Australia's fledgling research security framework, including by reference to documents obtained under the *Freedom of Information Act 1982* (Cth). Relevantly, Part II will examine the current role of the ARC in Australian research security, how it has previously attempted to research from national security risks, and the exposure of the limitation of the ARC's scope in recent inquiries and audits. Part III will then engage with how the ARC appears to have adjusted its national security posture following the PJCIS Inquiry. Part IV will then examine the role that *could* be played by the ARC, including by the introduction of tailored reforms and the enactment of new policy directions for the agency. Part V will present a brief conclusion.

II WHAT IS THE PROBLEM AND HOW HAS THE ARC DEALT WITH RESEARCH SECURITY?

The broad scope of problems facing universities can be summarised by reference to the report by the Center for Security and Emerging Technology ('CSET') on institutional research security of 2021.[20] At the interface between government and universities, there are problems of authority, information and trust, which on the one hand prevent the government from intervening or interfering in university

16 Ibid 120 [6.22].
17 Ibid 7 [2.10].
18 Ibid 37 [3.10].
19 Ibid 51 [3.61]–[3.62], Box 3.1.
20 Melissa Flagg and Zachary Arnold, *A New Institutional Approach to Research Security in the United States: Defending a Diverse R&D Ecosystem* (Policy Brief, January 2021) 2 <https://doi.org/10.51593/20200051>.

research arbitrarily, and on the other prevent properly informed collaboration between those two entities in response to national security risk on the other. The result – at least from a US standpoint, though the observations are salient for global university research – is a 'research enterprise is just too big, too distributed, too complex, and too exposed across too many sectors for a top-down, federally controlled approach to the research security challenge'.[21] The CSET called for a public-private partnership to be established as a clearinghouse for information and contextual, data-driven policy solutions that could involve co-designed responses from both government and academia.

From that perspective, the role of the ARC is a crucial one. It administers a significant proportion of the public funding of university research in Australia, which are awarded in circumstances where the national security risks to that research are not always well known or explored. Yet for the reasons that follow, the ARC has been largely unable to properly evaluate or examine applications for funding for national security threat, and so has been a significant gap in the Australian framework for protecting against those sources of risk.

A The Brief History of the ARC

The ARC was originally established under the *Employment, Education and Training Act 1988* (Cth)[22] as one of four separate councils intended to provide advice to the Minister for Education through the National Board of Employment, Education and Training ('NBEET'). The functions of the ARC (as originally established) included administration and distribution of grant funding under schemes referred to it, as well as to 'inquire into, and to provide information and advice to the Minister with respect to, any matter referred to the Council by the Minister'.[23] When the NBEET was abolished in 1996, the ARC continued to operate under its original legislative mandate, administering referred grant programs and issuing funding advice to the Minister about those programs.[24]

In 2001, the ARC became an independent statutory authority with the passing of the *Australian Research Council Act 2001* ('*ARC Act*'). Under the *ARC Act*, the ARC was established and constituted by the CEO, 'designated committees' and the staff of the ARC.[25] The ARC had the purposes of 'making of high quality recommendations to the Minister in relation to which research programs should receive financial assistance', administering those regimes of assistance and funding, and also providing 'high quality advice to the Minister about matters related to research'.[26]

---

21 Ibid 14.

22 *Employment, Education and Training Act 1988* (Cth) pt III.

23 Ibid ss 27(1)(a)–(b). Such inquiries could be conducted on the ARC's own initiative: at s 27(1)(c).

24 'A Brief History of the Australian Research Council', *Australian Research Council* (Infographic, June 2022) <https://www.arc.gov.au/sites/default/files/2022-06/Infograhic_preAct.pdf>.

25 *Australian Research Council Act 2001* (Cth) ss 5(1)–(2) ('*ARC Act*').

26 Ibid s 3, as inserted by *Australian Research Council Amendment Act 2006* (Cth) sch 1 item 1. Section 3 was later repealed by the *Australian Research Council Amendment (Review Response) Act 2024* (Cth) sch 1 item 1 ('*ARCARR Act*').

Whilst notionally an independent statutory agency, the ARC has courted controversy in the last two decades of its operation, largely due to the operation of the 'Ministerial veto'. The *ARC Act* permitted that the Minister 'may, in writing, approve a proposal for expenditure by an organisation (the approved organisation) on a research program (the approved program) as a proposal deserving financial assistance'.[27] As the *ARC Act* provided the Minister with a discretionary power, the Minister was at liberty to refuse to approve a research application for any reason, even in the face of strong recommendations by the ARC and its College of Experts.[28] This power was used relatively frequently by Ministers – Table 1 shows the Ministerial refusals of ARC funding applications since 2001.

Table 1: Grant Applications Refused by the Minister

Relevant Minister	Year	Number of Grants Refused
Hon Dr Brendan Nelson AO[29]	2004 2005	Three Seven
Hon Simon Birmingham MP[30]	2017 2018	Six Two
Hon Dan Tehan MP[31]	2021	Five
Hon Stuart Robert MP[32]	2022	Six

This generated a distinct sense of distrust between researchers and the Minister,[33] leading to some academics resigning from the ARC College of Experts in protest.[34] In response, the Minister announced on 30 August 2022 that an independent review of the ARC would be conducted with a 'broad' terms of reference, including the Ministerial power of veto ('*ARC Review Report*').[35] The *ARC Review Report* concluded that

27 Ibid s 53(1) (emphasis omitted), as repealed by the *ARCARR Act* (n 26) sch 3 item 6.

28 Previously, the *ARC Act* (n 25) s 52(4) stated the Minister 'may (but is not required to) rely solely on recommendations made by the ARC under subsection (1) of this section'. Amendments to the *ARC Act* (n 25) now provide an exhaustive list of criteria for approval of grants under section 48(3), including that the grant complies with approved funding rules, eligibility criteria and an appropriate assessment process.

29 Commonwealth, *Parliamentary Debates*, Senate, 15 February 2006, 15 (Peter Hoj).

30 Commonwealth, *Parliamentary Debates*, Senate, 25 October 2018, 184, 186 (Sue Thomas).

31 Commonwealth, *Parliamentary Debates*, Senate, 4 June 2021, 13–15 (Sue Thomas).

32 Commonwealth, *Parliamentary Debates*, Senate, 17 February 2022, 71 (Judi Zielke).

33 Stephen Matchett, 'La Trobe VC Challenges ARC over Research Cancellation' (29 October 2018) *Campus Morning Mail* <https://campusmorningmail.com.au/news/la-trobe-vc-challenges-arc-over-research-cancellation>; Natassia Chrysanthos, 'Eminent Researchers Condemn Government's "Political and Short-Sighted" Funding', *The Sydney Morning Herald* (online, 11 January 2022) <https://www.smh.com.au/national/eminent-researchers-condemn-government-s-political-and-short-sighted-funding-20220110-p59n2i.html>.

34 Andrew Francis and Aidan Sims, 'Why We Resigned from the ARC College of Experts after Minister Vetoed Research Grants', *The Conversation* (online, 2 February 2022) <https://theconversation.com/why-we-resigned-from-the-arc-college-of-experts-after-minister-vetoed-research-grants-175925>.

35 Jason Clare, 'Keynote Speech' (Speech, Australian Financial Review Higher Education Summit, 30 August 2022) <https://ministers.education.gov.au/clare/australian-financial-review-higher-education-summit-keynote-speech>.

'[i]n every iteration, Ministerial interventions have drawn international attention, and placed at threat the capacity of Australian researchers to form research links with international university and industry collaborators'.[36]

Relevantly to this article, the *ARC Review Report* also examined the role of 'national security issues' at the ARC.[37] The five rejections by Minister Tehan in 2021 outlined in Table 1 were reportedly for 'national security issues', which raised the spectre that 'this was potentially another form of political interference rather than the proper exercise of ministerial oversight of national security'.[38] The *Review* observed that the *University Foreign Interference Taskforce* ('UFIT') *Guidelines*, published by the Department of Education, had also been refreshed since those grant applications were dealt with.[39] The *Review* recommended that the Act 'contemplates a scenario for the Minister to exercise power in relation to national security concerns either for an application for funding or for a previously awarded grant, that is at any stage of the grant lifecycle', as well as providing scrutiny to the PJCIS.[40]

The *ARC Review Report* made ten recommendations on improving the ARC's governance, accountability and operating standards. Recommendation 5 suggested that the ARC Research Endowment Account ought to be utilised to administer the National Competitive Grants Program ('NCGP') consistent with a number of provisions, including:

> iv. the obligations of the ARC (i.e. Board and CEO) in relation to national security and NCGP are transparent; and that provision is made over and above these so the Minister may direct the CEO to not fund or to recover funds from grants made under the NCGP if the Minister were to become aware of national security concerns in relation to the grant or proposal. In the event of such a direction, the Minister must notify Parliament, stating the reasons for the direction; and/or report to the Parliamentary Joint Committee on Intelligence and Security or its successor where the security concern precludes the Minister reporting the detail of such a direction to Parliament.[41]

Importantly, the *ARC Review Report*'s authors were cautious not to empower the Minister above and beyond what was strictly necessary to address national security concerns, nor to use national security as a proxy for political interference. The recommendation was repeated in the executive summary to the extent that 'the Minister should retain the means to intervene in the extraordinary circumstance of a potential threat to national security', but where such intervention does occur, the intervention requires 'transparency and Parliamentary oversight'.[42]

---

36 Margaret Sheil, Susan Dodds and Mark Hutchinson, *Trusting Australia's Ability: Review of the Australian Research Council Act 2001* (Final Report, March 2023) ('*ARC Review Report*') 30 (citations omitted).

37 Ibid 32–5.

38 Ibid 32.

39 University Foreign Interference Taskforce, Department of Education, *Guidelines to Counter Foreign Interference in the Australian University Sector* (Report, 17 November 2021) <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector> ('*UFIT Guidelines*').

40 *ARC Review Report* (n 36) 33 (emphasis omitted).

41 Ibid 31.

42 Ibid 5.

The Government's response to the *ARC Review Report*, released in August 2023, was unequivocally supportive.[43] Recommendation 5 was noted as 'agreed', with amendments to the *ARC Act* to be made to enable the Endowment Account to be used in the recommended format. On 29 November 2023, the Australian Research Council Amendment (Review Response) Bill 2023 (Cth) was introduced, subsequently passing as the *Australian Research Council Amendment (Review Response) Act 2024* (Cth) ('*ARC Amendment Act*').[44] The *ARC Amendment Act* has potentially reshaped the ARC's role with respect to research security tasks, so I will return to these amendments later.

B How the ARC Has Previously Dealt with National Security Issues

The role of the ARC in terms of research security and dealing with national security issues has largely been reactionary. During the PJCIS Inquiry and when evidence emerged of Australian-based academics receiving ARC funding despite holding positions with foreign governments, the ARC indicated they were 'aware of some allegations against named researchers … but certainly [were] not fully aware of [others presented during the PJCIS Inquiry]'.[45] In response to questioning, the ARC freely indicated that it 'was not a national security specialist and required active engagement with stakeholders to identify and mitigate national security risks'.[46] That position remains despite the ARC dealing with applications for technology research which fall under the Commonwealth Government's *Blueprint and Action Plan for Critical Technologies* (including dual-use technologies)[47] and grants administered in conjunction with Australia's intelligence coordination agency, the Office of National Intelligence ('ONI').[48]

Previous activities by the ARC in this space were also canvassed by the PJCIS Inquiry. Historical processes allegedly involved 'scanning the media and checking internal ARC holdings', as well as seeking advice from the Department of Home Affairs.[49] Indeed, the five grant applications which were refused funding by Minister Tehan in 2021 were the first time that NCGP grants had been referred for national security advice. Researchers were also required to provide more in-depth information about foreign financial support and affiliations after amendments were made to the ARC's Conflict of Interest and Confidentiality Policy.[50] Certain circumstances also led to the ARC recovering grant funding from approximately

43 Australian Government, *Australian Government Response To: Trusting Australia's Ability* (Report, 22 August 2023).

44 The Bill received Royal Assent on 28 March 2024 and is now law, having taken effect on 1 July 2024.

45 *PJCIS Report* (n 15) 55 [3.73]. See also 52 [3.64].

46 Ibid 96 [4.80].

47 'List of Critical Technologies in the National Interest', *Department of Industry, Science and Resources* (Web Page, 19 May 2023) <https://www.industry.gov.au/publications/list-critical-technologies-national-interest> ('List of Critical Technologies in the National Interest').

48 'National Intelligence Community Research Program', *Office of National Intelligence* (Web Page) https://www.oni.gov.au/national-intelligence-community-research-program-grant-applications ('National Intelligence Community Research Program').

49 *PJCIS Report* (n 15) 96 [4.79].

50 Ibid 96–7 [4.82].

57 grants during the period 2016–2020, following allegations of 'expenditure on ineligible items, leaving the country for extended periods of time, or having a dual appointment'.[51]

What is apparent from the evidence presented at the PJCIS Inquiry is that the ARC was neither funded nor empowered sufficiently to conduct compliance monitoring on grants which it administered.[52] The PJCIS' conclusion was that 'while [the ARC] is not a national security specialist, it does need to properly audit these issues'.[53] By comparison, another body in higher education (the Tertiary Education Quality and Standards Agency ('TEQSA')) was also examined. Unlike the ARC, inspectors from the TEQSA are permitted to exercise compulsory powers to obtain information during compliance monitoring and investigations, and can seek search warrants in extreme cases.[54] Perhaps cognisant of that fact, the Committee recommended that the TEQSA be directed 'to initiate a regular audit of national security issues and responses in the sector by establishing a National Research Integrity Office'.[55]

The Committee then turned its attention to the role of the ARC and universities in applying for funding (whether under the NCGP or otherwise). The Committee's conclusion was that:

> … substantial improvements are required on the topic of ARC grant provision, audit and disclosure. This is an area that has 'slipped' between the gaps with the ARC saying it is the responsibility of the universities, and universities saying it is too difficult to do disclosure on their academics who are partially disclosing their affiliations. This is not satisfactory and a clear national security risk that requires immediate remediation.[56]

In drawing that conclusion, the PJCIS made three recommendations which had the potential to impact the ARC's research security role:

- Recommendation 19 was to commission a risk-based audit of grants as well as investigating the adequacy of existing penalties for breaches of the ARC Grant Rules;[57]
- Recommendation 26 for the ARC to communicate to the sector (via UFIT) the serious penalties for grant fraud 'and prioritise investigation and enforcement of them';[58] and
- Recommendation 27 to conduct 'a review of the ARC's performance in assessing foreign interference and national security risks in the context of grant decisions'.[59]

Interestingly, at the time of writing, recommendation 19 has not been completed. This recommendation – that '[t]he Department of Education will engage with

51 Ibid 97 [4.84].
52 Ibid 98 [4.87].
53 Ibid 139 [6.121].
54 *Tertiary Education Quality and Standards Agency Act 2011* (Cth) ss 115–16, referring to and applying the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) pts 2–3.
55 *PJCIS Report* (n 15) 135 [6.100].
56 Ibid 138 [6.115].
57 Ibid 133–4 [6.92].
58 Ibid 139 [6.118].
59 Ibid 139 [6.120].

the Australian Research Council ('ARC') to review active/current ARC grants in the context of consideration of foreign interference risks since the launch of the original *UFIT Guidelines*' – was supported-in-principle.[60] Yet enquiries to the Department about the report of that review show the Department 'is unaware of any report resulting from recommendation 19 of the Inquiry'.[61] Recommendation 26 appears – such as it was made – to be an ongoing action of the UFIT to continue to raise awareness of the penalties for grant fraud. The Government's response was that it was otherwise satisfied with 'existing penalties appropriate for breaches of ARC grant rules' and 'ARC compliance arrangements'.[62]

C The Five Refused Grants

As was discussed in Part I, then-Minister for Education Dan Tehan exercised his discretion not to approve funding to five grants in the 2021 funding round. All five grants were applications under the ARC's Discovery Research Project stream and involved requests for funding over a three-year timeframe. The five grants outlined in Table 2 were part of a broader group of 18 grant applications which were referred to the Department of Home Affairs for advice. Based (either in part or in full on that advice) the Minister declined to fund all five grants.

Table 2: Five ARC Discovery Grants Not Funded for National Security Reasons in 2021 Funding Round[63]

Host University	Title	Funding Requested (Over 3 Years)
Australian National University	Spatiotemporal Light Control Using Programmable Organometallics	AUD 589,000
Australian National University	Hybrid Exciton-polariton Lasers based on 2D Organic-Inorganic Materials	AUD 495,024
University of Technology, Sydney	Steerable Multi-Beam Leaky Wave Antennas for Wireless Communications	AUD 450,436
Queensland University of Technology	Advanced data-driven battery models and architectures for resilient grids	AUD 378,585
University of Southern Queensland	High-Temperature Proton-Conducting Composite Membrane for Advance Fuel Cell	AUD 395,000

60 Australian Government, *Australian Government Response to the Parliamentary Joint Committee on Intelligence and Security Report: National Security Risks Affecting the Australian Higher Education and Research Sector* (Report, February 2023) 10 <https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/government-response-national-security-risk-affecting-higher-education-research-sector.pdf> ('*PJCIS Response*').

61 A copy of this correspondence is on file with the author.

62 *PJCIS Response* (n 60) 10.

63 A copy of this document was obtained under *Freedom of Information Act 1982* (Cth) ('*FOI Act*') from the Australian Research Council ('ARC') and is on file with the author.

The nature of the national security risk is not immediately apparent from the titles of these projects alone, and requests for more detailed information on four of the five grants by the author was refused by the ARC on the basis that the documents contained 'material obtained in confidence',[64] information with commercial value,[65] could disclose the business affairs of an organisation,[66] and would 'be likely unreasonably to expose the agency or officer [ANU] to disadvantage'.[67] However given that the scope of the freedom of information request was for 'Part D Project Descriptions of the applications in the NCGP rejected on the basis of national security grounds', it must be concluded that no further grants have been refused by the Minister on the grounds of national security concerns since those in Table 2.

III HOW RESEARCH SECURITY CHANGED AFTER THE PJCIS INQUIRY

Surprisingly, the Government's response to the PJCIS Inquiry was quite tepid. Of the 27 recommendations of the PJCIS, 12 were supported, nine were supported-in-principle only, five were noted and one was not supported.[68] Both of the recommendations which applied substantially to the ARC's operations (recommendations 19 and 26) were only supported-in-principle, with the Government concluding that penalties for breaches of grant rules were 'appropriate' and that communication regarding grant fraud through UFIT was already 'ongoing'.[69]

Yet the PJCIS Inquiry had heard evidence that the ARC was attempting to broaden its exposure to national security agencies, commencing in 2018 with the ASIO and followed by the Department of Home Affairs in 2020. What was limiting the collaboration between the ARC and these agencies at that time was the legal communication and sharing of information without infringing various secrecy provisions.[70]

Beyond those interactions, the ARC has held responsibilities for identifying key national security risks in the NCGP since at least 2019. Examination of grant applications for the possibility of foreign interference risks has been largely limited to those technologies listed on Australia's *Blueprint and Action Plan for Critical Technologies*.[71] Any adverse findings are – at least for the present time – raised with universities to resolve, given that the functions of the ARC[72] and its CEO are solely to 'make recommendations to the Minister … in relation to which

64 *FOI Act* (n 63) s 45.
65 Ibid s 47(1)(b).
66 Ibid s 47G(1).
67 Ibid s 47H(b). A copy of the decision letter from the ARC is on file with the author.
68 *PJCIS Response* (n 60).
69 Ibid 10, 12.
70 *PJCIS Report* (n 15) 96 [4.81].
71 List of Critical Technologies in the National Interest (n 47).
72 Solely 'to assist the CEO in the performance of the CEO's functions': *Australian Research Council Act 2001* (Cth) s 6.

proposals should be approved as deserving financial assistance … to administer [those] regimes of financial assistance … [and] to provide advice to the Minister on research matters'.[73]

A The Amended Guidelines to Counter Foreign Interference in the Australian University Sector and *Collaborate with Care*

After the PJCIS Inquiry had finalised its public hearings but before the public release of its final report, the *UFIT Guidelines* were refreshed by the Department of Education.[74] During the consultation phase, the *UFIT Guidelines* were criticised for adopting 'mandatory language' to impose 'formalised regulation and higher compliance requirements',[75] as well as adopting 'a new and unnecessary tone of instruction and direction that is inconsistent with the text produced in the collaborative phase, and that is more appropriate to a legislative instrument than a set of guidelines'.[76] Then, in 2023, ASIO produced the *Collaborate with Care* booklet,[77] listing a series of risks (and actions that could be taken to minimise those risks) involved in international collaboration. The release of this resource was not very highly publicised and is not universally referenced in funding applications (other than those co-administered by the ONI).[78]

Further, both the *UFIT Guidelines* and *Collaborate with Care* are voluntary – these documents do not impose mandatory obligations on universities nor any baseline standards necessary to achieve those obligations. A report commissioned by the Government in August 2023 found that the understanding of national security risks and maturity in responding under the *UFIT Guidelines* varied wildly across the university sector.[79] The *UFIT Guidelines* are also somewhat myopic: by focusing attention solely on foreign interference, they risk blinding researchers and research institutions to the full range of national security risks to university research (including espionage, intellectual property theft and 'quasi-legal' actions such as predatory publications and patenting). Despite recommendation 26 of the PJCIS Inquiry also concluding that '[t]enders issued by all government agencies providing grants to research institutions should include a standard clause requiring compliance with existing countering foreign interference policies', this

---

73 Ibid s 33B, later amended by *ARCARR Act* (n 26) sch 2 items 13–18, sch 3 items 4–5.

74 *UFIT Guidelines* (n 39).

75 University of Melbourne, Submission to Department of Home Affairs, *Consultation Draft of the Guidelines to Counter Foreign Interference in the Australian University Sector* (6 September 2021) 6 <https://about.unimelb.edu.au/__data/assets/pdf_file/0019/312247/UFIT-refresh_UoM-response.pdf>.

76 Queensland University of Technology, Submission to Department of Home Affairs, *Consultation Draft of the Guidelines to Counter Foreign Interference in the Australian University Sector* 1 <https://cms.qut.edu.au/__data/assets/pdf_file/0016/1202551/qut-submission-ufit-guidelines-refresh.pdf>.

77 Australian Security Intelligence Organisation, *Protect Your Research: Collaborate with Care* (Booklet, May 2023) <https://bjbs-news.csu.edu.au/wp-content/uploads/sites/4/2023/05/Protect-Your-Research-Collaborate-with-Care-Booklet.pdf> ('*Collaborate with Care*').

78 National Intelligence Community Research Program (n 48).

79 Department of Education, *Report on Implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector* (Report, 24 August 2023) <https://www.education.gov.au/download/16827/report-implementation-guidelines-counter-foreign-interference-australian-university-sector/34097/document/pdf> ('*2023 Implementation Review*').

recommendation was only supported-in-principle[80] and it remains unclear whether on publicly available information this recommendation has been fully implemented by the ARC.

The imposition of obligations on universities seeking NCGP funding to demonstrate, or at least make a formal declaration, that they meet the minimum standard of compliance with the *UFIT Guidelines* would be extremely useful in reducing the 'attack surface' for foreign agents. By telegraphing the requirements publicly, the ARC could play a role in clearly demonstrating that a higher standard of diligence applies to research institutions under the NCGP.[81] Equally, the imposition of those standards could increase transparency around grant funding and grant utilisation and reporting, in turn addressing the PJCIS Inquiry's concerns around grant fraud.[82] And requiring universities to perform appropriate standards of due diligence on possible researchers may also have the effect of meeting those institutions individual obligations around safe and secure workplaces.[83]

Such imposition could also help universities meet their cybersecurity obligations imposed by other laws. For example, most (if not all) universities operate 'critical education assets' under the *Security of Critical Infrastructure Act 2018* (Cth)[84] and are part of a 'critical infrastructure sector' with 'critical infrastructure assets'.[85] Meeting research security standards could assist universities in auditing and monitoring their data access and security policies, in turn enabling more rapid detection of problems which would invoke their notification and cyber incident reporting requirements.

B *ARC Work Instructions* for Pre- and Post-Award

Since the PJCIS Inquiry, the ARC itself seems to have been actively looking to strengthen its security posture. An audit was conducted by McGrathNicol in March 2023 by the ARC pursuant to the PJCIS recommendation 27, with a focus on examining the ARC's processes in the handling of foreign interference risk.[86] This audit made three recommendations around the ARC's processes, including the consideration of implementing 'follow up checks' for grants that previously displayed security risks, and 'spot checks' on grants for ongoing compliance. Although these checks still appear to be a work in progress, the ARC did re-issue work instructions in August 2022 (updated in May 2023) for *Countering*

80 *PJCIS Response* (n 60) 12.

81 Suzanne Folsom and Robert Garretson, 'The Continuing Danger of Academic Espionage', *Inside Higher Ed* (online, 4 May 2020) <https://www.insidehighered.com/views/2020/05/05/threat-academic-espionage-should-not-be-overlooked-even-time-pandemic-opinion>.

82 Ibid.

83 Aleta Wilson and Clay Wilson, 'The Effects of US Government Security Regulations on the Cybersecurity Professional' (2011) 15(2) *Proceedings of the Academy of Legal, Ethical and Regulatory Issues* 5 <https://www.abacademies.org/Public/Proceedings/Proceedings29/ALERI%20Proceedings%20Fall%202011.pdf>.

84 *Security of Critical Infrastructure Act 2018* (Cth) s 5. This includes the Australian National University as well under the *Security of Critical Infrastructure (Australian National University) Rules (LIN 22/041) 2022* (Cth).

85 Ibid ss 8D, 9(1)(dk), 9(1)(dk).

86 A copy of this document was obtained under the *FOI Act* (n 63) and is on file with the author.

Foreign Interference Checks for Pre-Award Applications and Countering Foreign Interference for Post-Award Variations ('*ARC Work Instructions*').[87] These checks apply to all applications recommended for funding from the commencement date of the instructions.

The *ARC Work Instructions* turn attention to three key grounds of risk: critical technology, people and organisations. If the research application contains references to an application in the field of critical technology (as established by the List of Critical Technologies in the National Interest),[88] then the application will be considered 'sensitive' and raised for review with the Due Diligence Committee ('DDC') of the ARC.[89] Equally, associations between applicants for funding and foreign organisations, entities or agencies must also be reviewed to identify applicants with ongoing financial or other affiliations or associations with non-Australian governments or entities.[90] The ARC also confirms that applicants and their research partners have not been the subject of sanctions by Australia and/or the United Nations ('UN') Security Council. The same checks are conducted on applications where new persons or organisations are added to the application post-award.

There are several shortfalls observable from the current processes for screening grant applications. The first is that affiliations between applicants for research grants and their partner institutions are limited solely to the information supplied by the university during the application process. Although the ARC gave evidence to the PJCIS that they had updated their Conflict of Interest and Confidentiality Policy in late 2020 to capture a wider range of affiliations (such as 'financial support … sponsored talent programs, governments, political parties, state-owned enterprises, military or policy organisations as part of their declaration of material personal interests),[91] there is no additional or supplementary form of assessment to identify entities behind that which is prima facie disclosed. The *Report on Implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector* ('*2023 Implementation Review*') demonstrated empirically that some universities were struggling to fully service the due diligence disclosure requirements.[92] Further, there are reports that even despite these improvements, security-critical research is still not being adequately disclosed.[93]

87 A copy of each document was obtained under the *FOI Act* (n 63) and is on file with the author.

88 List of Critical Technologies in the National Interest (n 47). See also *Migration (Critical Technology—Kinds of Technology) Specification (LIN 24/010) 2024* (Cth) ss 4–5.

89 The Due Diligence Committee ('DDC') will then determine what action to take, including referring the application to Home Affairs for checking, seeking further information from the host universities, or continue with a funding recommendation to the CEO.

90 Such as by checking the Australian Strategic Policy Institute's *China Defence Universities Tracker* (n 5).

91 *PJCIS Report* (n 15) 96–7 [4.82].

92 *2023 Implementation Review* (n 79) 13.

93 For example, a project involving 'use of drones – known as unmanned aerial vehicles ('UAVs') – in wireless networks and as communications hubs' was instigated between the University of New South Wales, the University of Houston and Sharif University of Technology in Iran: Jonathan Yerushalmy and Johana Bhuiyan, 'Academics in US, UK and Australia Collaborated on Drone Research with Iranian University Close to Regime', *The Guardian* (online, 15 February 2024) <https://www.theguardian.

Secondly, although the ARC is clearly screening sanctions imposed by the UN Security Council or Australia under the *Autonomous Sanctions Act 2011* (Cth) ('*Autonomous Sanctions Act*'),[94] this screening does not reference other publicly available 'sanctions' such as those published on the US Entity List,[95] the Japanese Ministry of Economy, Trade and Industry end user list,[96] or Canada's 'Named Research Organisations'.[97] The utility of these lists is the lower threshold they take to illicit conduct, such that they incorporate foreign entities which pose security risks but have not engaged in conduct which exposes them to liability for sanctions under international law. For example, entities may be listed on the US Entity List are included where the End-User Review Committee ('ERC') concludes the entity 'engaged in activities contrary to [US] national security and/or foreign policy interests'.[98]

The third limitation of the *ARC Work Instructions* is that they do not necessarily reflect best international practice. For example, under the *National Security Guidelines for Research Partnerships* ('*Canada Guidelines*')[99] – which have applied to all funding sought from the Canadian Government since 2019 – grant applicants must perform risk assessments on foreign partners as a prerequisite for funding. These assessments consider two elements of risk when determining compliance: (a) '[r]esearch area: what are you working on?'; and (b) '[r]esearch partner: who are you working with?'[100] Canadian researchers that conduct research in 'Sensitive Technology Research Areas' are also obligated to check the affiliations of any research entities to ensure they do not have any connections with the Named Research Organization List.[101] ARC grant applications do not require the completion of national security risk assessments in any applications, nor do they oblige individual researchers to check named lists of entities that pose national

com/world/2024/feb/14/academics-in-us-uk-and-australia-collaborated-on-drone-research-with-iranian-university-close-to-regime>.

94 Including those available in 2021 under the *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021* (Cth).

95 Published as Supplement No 4 to Part 744 of the *Export Administration Regulations*, 15 CFR § 744 (1996) ('*US Entity List*').

96 'Review of the End User List', *Ministry of Economy, Trade and Industry* (Web Page, 4 November 2022) <https://www.meti.go.jp/english/press/2022/1104_002.html>.

97 Published under the Innovation, Science and Economic Development Canada, *Policy on Sensitive Technology Research and Affiliations of Concern* (Report, 9 January 2024) <https://ised-isde.canada.ca/site/science/sites/default/files/documents/2024-01/1154-policy-strac-en-final-09Jan2024.pdf> ('*Policy on Sensitive Research and Affiliations*'). See Innovation, Science and Economic Development Canada, *Named Research Organisations* (Report, January 2024) <https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1082-named-research-organizations-list-09Jan2024.pdf>.

98 *US Entity List* (n 95) § 744.11.

99 Innovation, Science and Economic Development Canada, *National Security Guidelines for Research Partnerships* (Guidelines, 2024) <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships> ('*Canada Guidelines*').

100 Ibid 7–8.

101 *Policy on Sensitive Research and Affiliations* (n 97).

security risks (though the ARC may conduct follow-up enquiries with universities and researchers where their application raises national security concerns).[102]

C The ARC Countering Foreign Interference Framework

Running alongside the work instructions above, the ARC has also issued a *Countering Foreign Interference Framework* ('*CFI Framework*'),[103] which applies at each stage of the consideration of grants under the NCGP. The predominant focus of due diligence assessments under the *CFI Framework* are imposed on universities, where 'risk assessments undertaken as outlined in the *UFIT Guidelines* and UFIT Due Diligence Framework'.[104] Universities are also responsible for ensuring that appropriate risk mitigation strategies are in place prior to the grant application being submitted to the ARC. The ARC then conducts its own due diligence reviews (no doubt in accordance with the ARC work instructions), particularly in relation to applications relating to critical technologies. Issues may include 'foreign financial support … foreign talent program[s] … associations with a foreign government, military, policing or intelligence organisation … [or] association with a regime, person or organisation with which Australia has sanctions in place'.[105] Where issues are identified, the university or national security agencies may be involved – again, a decision dependent on the views of the ARC's DDC.

One obvious difficulty for universities (and the ARC as well) in this model is that by carrying the compliance burden at the outset, universities are largely operating in the dark when it comes to the activities of foreign entities. Universities are not permitted access to security intelligence that may be available on a given foreign researcher or research entity (beyond publicly available information).[106] Indeed, the PJCIS Inquiry concluded that '[t]he Committee does not accept that it is an absence of Australian government intelligence that is preventing the sector from undertaking proper due diligence'.[107]

There is some validity to that position. Disclosure of security intelligence carries a risk that it could permit identification and quantification of intelligence capabilities as well as preventing or foreshadowing ongoing or future activities by ASIO and its partners in the National Intelligence Community. This was the specific reason given for the Government's rejection of recommendation 10 in the PJCIS Inquiry for ASIO to report annually on security risks to higher education.[108] Disclosing security intelligence to universities also runs the risk that such

---

102 'Countering Foreign Interference', *Australian Research Council* (Web Page, 2022) <http://web.archive.org/web/20240323231421/https://www.arc.gov.au/funding-research/research-security/countering-foreign-interference>.

103 Australian Research Council, *ARC Countering Foreign Interference Framework* (Guide, December 2023) <https://www.arc.gov.au/sites/default/files/2023-12/ARC%20Countering%20Foreign%20Interference%20Framework.pdf>.

104 Ibid 6.

105 Ibid.

106 ASIO employees cannot share information they gather or hold without the authority of the Director-General: *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18–18B ('*ASIO Act*').

107 *PJCIS Report* (n 15) 129 [6.65]

108 Ibid 127 [6.54]; *PJCIS Response* (n 60) 6.

information could be subpoenaed or otherwise disclosed as part of tribunal or court proceedings. Whilst there is a statutory framework that specifically permits orders to be made that restricts the admissibility and treatment of classified information,[109] the risks cannot be neutralised.

IV THE FUTURE POTENTIAL FOR THE ARC AND RESEARCH SECURITY

Australian society has long recognised that the imperative to protect the sanctity of university teaching and research is not just a legal obligation, but a moral and ethical one as well. As Kirby J said in *Griffith v Tang*:

> The maintenance of high standards of teaching and research, and the furtherance of the export of university services by Australian universities, make it essential that public regulation of universities be scrupulously maintained, in accordance with the law enacted to achieve that objective. It also makes the defence of academic standards and of the integrity of degrees or awards and university research a vital part of the functions of such statutory bodies.[110]

Within that public regulation framework, the ARC has enormous potential to play an increased role because of its gatekeeping role to the funds administered under the NCGP. Whilst universities might continue to self-fund and seek third-party funding, a failure to comply with the requirements of increased scrutiny of grant applications by the ARC would effectively 'lock out' those institutions from the prestigious awards the ARC administers.

There are other ancillary benefits to using the ARC as a regulatory mechanism for national security. Rather than applying individual penalties for contraventions which may or may not be detected – such as export control and secrecy laws do – meeting baseline standards as a condition of grant funding promotes the uplifting of security standards. The risk associated with losing reputation as a top-flight research university could well be enough to motivate most institutions.[111]

Internationally, there are growing calls for funding bodies to play a greater role in the secure administration of university research. In 2019, the JASON Group called for harmonisation of rules across the funding agencies consistent with guidelines put out by the National Science Foundation.[112] In 2020, the Swedish Foundation for International Cooperation in Research and Higher Education published a report on 'responsible internationalisation' which concluded '[r]esearch funders that support international cooperation should also be able to request … risk assessments to ensure

---

109 See, eg, *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 19.

110 *Griffith University v Tang* (2005) 221 CLR 99, 120 [107] (Kirby J).

111 With one US research manager quoted as saying '[it's] not the fine; it's our institutional integrity. We would lose so much more than those fines in our credibility as a research institution, in our ability to do research and get funding for our research': John Krige, 'National Security and Academia: Regulating the International Circulation of Knowledge' (2014) 70(2) *Bulletin of the Atomic Scientists* 42, 48 <https://doi.org/10.1177/0096340214523249>.

112 Gordon Long, *Fundamental Research Security* (Report No JSR-19-2I, 6 December 2019) 3 <https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf>.

that the necessary measures are taken to ensure responsible internationalisation'.[113] Research funding groups in the US have even suggested forming their own clearinghouse for sharing information about risky research entities and their practices.[114] Nor are these calls absent any empirical basis. Studies by the Swedish Foundation for International Cooperation in Research and Higher Education have continually raised the importance of funding bodies ensuring 'governance mechanisms that integrate research integrity, research security, research ethics and responsible internationalization'.[115] These studies continue to highlight the need for the incorporation of 'reciprocity' – the notion that researchers should enjoy mutual benefits, influence and protections as outcomes of the research (as opposed to one-sided or uneven benefits for the parties).[116]

If one takes a holistic view across both the *ARC Review Report* and the *2023 Implementation Review*, it is easy to see a number of areas where the ARC could take the lead role in ensuring research security standards. As Shih outlined in their work on research funders, this would involve the ARC deepening their maturity and resilience in four key areas:[117]

- Identifying pertinent issue sets;
- Focusing on the relationship level;
- Focusing on agency rather than compliance; and
- Understanding the nature of reciprocal exchanges.

A Applying an Increased Research Security Role of the ARC

As was established earlier, universities are not always best placed to identify the potential issues in relation to national security risk, where they have a vested interest in both the conduct of research and its internationalisation and commercialisation. Yet this offers opportunities for accurately delineating the roles of due diligence between those issues of concern at the institution level and those issues at the strategic (ie, ARC) level. For example, a university may demand local storage of research data in a domestic, non-cloud-based source with access restricted to local researchers and support staff to protect its intellectual property.[118] This has duplicate

113 Tommy Shih, Albin Gaunt and Stefan Östlund, *Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration* (Report, 2020) <https://www.stint.se/wp-content/uploads/2020/02/STINT__Responsible_Internationalisation.pdf>.

114 Richard L Hudson, 'National Science Funders Eye Setting Up International Network to Share Research-Security Information', *Science | Business* (online, 12 December 2023) <https://sciencebusiness.net/news/international-news/national-science-funders-eye-setting-international-network-share-research>.

115 Tommy Shih, 'The Role of Research Funders in Providing Directions for Managing Responsible Internationalization and Research Security' (2024) 201 *Technological Forecasting and Social Change* 123253:1–10, 4 <https://doi.org/10.1016/j.techfore.2024.123253>. See also Tommy Shih, 'Recalibrated Responses Needed to a Global Research Landscape in Flux' (2024) 31(2) *Accountability in Research* 73 <https://doi.org/10.1080/08989621.2022.2103410>.

116 Shih, 'The Role of Research Funders in Providing Directions for Managing Responsible Internationalization and Research Security' (n 115) 6–7.

117 Ibid 8.

118 For example, consider the recent announcement of the NEBULA project between CyberCX and Curtin University: CyberCX, 'CyberCX Partners with Curtin University to Launch Sovereign Cloud Platform for Sensitive Research' (Media Release, 1 August 2024) <https://cybercx.com.au/news/nebula-launch>.

benefits for research security by ensuring that data is only accessible where the host institution can exercise the majority of its risk management influence.

Both universities and the ARC need to identify wider and more diverse sources of open-source information on which to base their due diligence activities. For example, the *ARC Work Instructions* referred to the Australian Strategic Policy Institute's *China Defence Universities Tracker*, an online database of Chinese universities connected to military, intelligence or security apparatus of the Chinese Communist Party. However, this database is now five years old, and only applies to Chinese entities and not the full gamut of potential 'risky' countries (ie, it does not list Russian, Iranian or North Korean institutes of concern). Instead, more regularly updated lists such as the US and Japanese Entity Lists, and Canadian Named Research Organizations list could be used.

At the same time, the ARC may need to embrace some exposure to classified information in the pursuit of its statutory objectives to provide 'high quality advice to the Minister about matters related to research'.[119] The view of the PJCIS that 'universities do not need classified intelligence' does not strictly apply to the ARC. As a Commonwealth government agency, there is no reason that the ARC could not be permitted to share in the classified intelligence available to agencies like the Department of Home Affairs and ASIO on a more permanent, ongoing basis. This would require a specific statutory amendment to achieve, and possibly involve resource implications to uplift the security of the ARC and the training of its staff in relevant procedures. Alternatively, an officer of ASIO with dedicated access to their security intelligence could be embedded or seconded to the ARC to achieve the same effect (similar to the security precautions being applied to Defence ahead of the transfer of nuclear propulsion technology under the AUKUS agreement).[120]

The *ARC Review Report* likewise appears to support the active consideration of these forms of intelligence when considering not to approve funding a grant application because of national security concerns. Not only would this be a necessary implication where '[the] ARC, CEO and Board have on-going obligations in respect to national security',[121] but because the *ARC Review Report* recommended that the Ministerial veto only be permitted 'in rare cases [where] the Minister may be made aware of concerns with a sufficient urgency or high-level of secrecy that cannot be shared with the Board, CEO, or university'.[122]

The ARC likely needs to educate researchers that these obligations exist across the funding lifecycle. This would include imposing a contractual requirement on universities receiving NCGP funding to report security incidents (which in turn, requires frameworks and policies capable of yielding them for discovery).

---

119 *ARC Act* (n 25) s 3(a)(iii), as inserted by *Australian Research Council Amendment Act 2006* (Cth) sch 1 item 1. Section 3(a)(iii) was later repealed by *ARCARR Act* (n 26) sch 1 item 1.

120 Matthew Knott, 'ASIO Agents Embedded in Defence to Protect AUKUS Secrets from Foreign Spies', *The Sydney Morning Herald* (online, 23 May 2023) <https://www.smh.com.au/politics/federal/asio-agents-embedded-in-defence-to-protect-aukus-secrets-from-foreign-spies-20230523-p5danc.html>.

121 *ARC Review Report* (n 36) 33.

122 Ibid.

Despite the known risks, universities often display reactive security mindsets.[123] Researchers often think they are not of interest to intelligence and security actors, such that 'threats and vulnerabilities are generally not considered until after a security breach has occurred'.[124] Unusual, repetitive or odd requests for academic collaboration or opinion, or unexplainable requests for anonymity should be notified to ASIO, along with all forms of cybersecurity incidents involving research data.[125] Reporting approaches by foreign security forces, police, diplomatic personnel or other suspicious characters should also be a *fait accompli* for travelling academics and student exchanges.[126]

B Focusing on the Primacy of Relationships and Agency

One of the best ways the ARC could take a more active role in the facilitation of universities achieving compliance with global best practice in the protection of their research endeavours is focusing on building relationships and agency across the university sector. In particular, this would involve development of new funding measures along the same lines as the *Canada Guidelines*, which in turn calls for a broader, more consistent government policy on research security. Alternately, it could involve the establishment of a clearinghouse as recommended by CSET and as recently exemplified by the Safeguarding the Entire Community of the US Research Ecosystem ('SECURE') Center between the National Science Foundation, University of Washington and Texas A&M University.[127]

Perhaps the simplest, cheapest upfront fix – and consistent with Recommendation 26 of the PJCIS Inquiry – could take the form of a mandatory declaration at the grant application level where both universities and individual researchers attest that: they are aware the *UFIT Guidelines* apply to their work; that they are aware of the institutional policies around those guidelines; and that they have received training in handling and reporting matters which may touch on national security issues. Of course, existing declarations for similar disclosures provisions (such

123 Debora Halbert, 'Intellectual Property Theft and National Security: Agendas and Assumptions' (2016) 32(4) *The Information Society* 256 <https://doi.org/10.1080/01972243.2016.1177762>.

124 Tim Lane and Lauren May, 'Improving Information Security Management: An Australian Universities Case Study' in Katina Michael and MG Michael (eds), *The Second Workshop on the Social Implications of National Security: From Dataveillance to Überveillance and the Realpolitik of the Transparent Society* (University of Wollongong, 2007) 281, 288. See also Andrew G Kotulic and Jan Guynes Clark, 'Why There Aren't More Information Security Research Studies' (2004) 41(5) *Information and Management* 597 <https://doi.org/10.1016/j.im.2003.08.001>; Bongiovanni (n 12).

125 *Collaborate with Care* (n 77).

126 Daniel Golden, 'How the CIA Staged Sham Academic Conferences to Thwart Iran's Nuclear Program', *ProPublica* (online, 10 October 2017) <https://www.propublica.org/article/spy-schools-how-the-cia-staged-sham-academic-conferences-to-thwart-iran-nuclear-program>; Cécile Fabre, *Spying Through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence* (Oxford Academic Press, 2022) 142–173 <https://doi.org/10.1093/oso/9780198833765.001.0001>.

127 US National Science Foundation, 'NSF-Backed SECURE Center Will Support Research Security, International Collaboration' (Media Release, 24 July 2024) <https://new.nsf.gov/news/nsf-backed-secure-center-will-support-research>.

as conflicts of interest)[128] are already in place and are of dubious utility where researchers are already being asked to self-assess for compliance.

Alternatively, where an application involves a technology on the *Blueprint and Action Plan for Critical Technologies*, the ARC may take more of an auditing role in which they require a university to supply evidence of:

- That university's corporate experience (if any) in dealing with high-risk or classified research;[129]
- The institution's policies which protect research security, academic freedom, institutional autonomy, freedom of expression and equity, diversity, and inclusion in its research agenda;[130]
- How the institution classifies, assessing and managing research conducted 'in the national interest';[131]
- The institution's staff and students have, or will be, suitably trained and competent to identify and manage national security risks in the course of their work.

Another option could involve the conferral of the regulatory powers vested in TEQSA on the ARC. This could perhaps be a more acceptable option to the Government given that one of the PJCIS recommendations was for a National Research Integrity Office to be established within TEQSA,[132] but the Government's response rejected that notion.[133] However, it would fundamentally challenge the entire nature of the ARC (and require substantial legal reform) for them to be vested with prima facie law enforcement responsibilities when the listed statutory objects of the ARC limit the agency's remit to funding decisions and advisory duties to the Minister. There would likely be pushback from the sector to consider, which has previously railed against increased burdens or 'red tape', even in the presence of national security threats.[134] Such calls are not always unjustified; the

128 See, eg, conflicts as required by the ARC's Conflict of Interest and Confidentiality Policy: *PJCIS Report* (n 15) 96–7 [4.82].

129 Adapted from the *Canada Guidelines* (n 99) 10.

130 Ibid 5–6.

131 For present purposes this includes research with military applications or subject to export controls, research into dual-use technologies (not otherwise subject to export control), and research carrying a security classification or involving the Australian National Intelligence Community.

132 *PJCIS Report* (n 15) 135 [6.100].

133 Saying 'TEQSA's establishing framework does not extend to the required legislative remit, capacity or expertise to deliver on addressing this recommendation': *PJCIS Response* (n 60) 11.

134 Fred Hilmer, 'Over-Regulation of Universities Stifles Innovation', *University New South Wales Newsroom* (online, 4 March 2013) <https://newsroom.unsw.edu.au/news/general/over-regulation-universities-stifles-innovation>; Paul Karp, 'Universities Blindsided by Dan Tehan's Plan for Integrity Unit to Monitor Enrolments', *The Guardian* (online, 25 June 2020) <https://www.theguardian.com/australia-news/2020/jun/25/universities-blindsided-by-dan-tehans-plan-for-integrity-unit-to-monitor-enrolments>; Group of Eight Australia, 'Go8 Statement on Australian Foreign Relations Bill' (Media Release, 27 August 2020) <https://go8.edu.au/go8-statement-on-australian-foreign-relations-bill>; Group of Eight Australia, *Essential Decisions for National Success: Reducing the Regulatory Overload on Our Universities* (Report, 2 May 2022) <https://go8.edu.au/report-reducing-the-regulatory-overload-on-our-universities>; Julie Hare, 'Scientists Risk Jail for Sharing Research outside AUKUS', *Australian Financial Review* (online, 19 November 2023) <https://www.afr.com/policy/foreign-affairs/scientists-risk-jail-for-sharing-research-outside-aukus-20231117-p5ekty>.

optics of conferring a funding agency with powers akin to those of a police force would be hard to square and may cause both cost and resource implications for higher education institutions, or budget cuts or restrictions for other aspects of the university experience. Because the ARC would still need to be the administration body for funds under the NCGP, there is also the strong possibility of regulatory capture, with the ARC having to balance funding universities on the one hand and acting as their regulator on the other.

The last existing option involves the cultivation of a closer working and legal relationship between ARC and ASIO. ASIO possesses both the expertise and legislative remit to uplift and assist the ARC's provision of research security. For example, the ARC may – as an 'agency' which administers Commonwealth funds as one of its statutory objectives – be permitted to request 'security assessments relevant to their functions and responsibilities',[135] ie, NCGP grant applicants. This would permit ASIO to investigate the full range of national security risks of grant applicants, including not only foreign interference but also espionage, sabotage, politically motivated violence, promotion of communal violence, or attacks on Australia's defence system.[136]

This is a proposal likely to need statutory clarity and would benefit from the public comment and consultation such amendments would inevitably require. The question of resourcing would also need to be answered. When ASIO took over the conduct of 'Positive Vetting' security clearances from the Department of Defence in 2023, a budgetary increase was also given to ASIO in recognition of the workload involved in these clearances.[137] Again, the university sector is unlikely to be happy with such a proposal, and the intelligence agency itself may also have a view that such activities might unnecessarily expose their methodologies or technologies to unwanted and unnecessary scrutiny.[138]

A more technical-focused solution could also be explored between the ARC and ASIO. Rather than ARC being required to maintain security-cleared infrastructure and personnel, and handle the information supplied to it by ASIO, there could instead be a digital clearinghouse for the ARC to refer grant applicants (and their research partners) in a similar manner to how criminal history checks are conducted[139] (an adapted model is shown in Figure 1). An application – consisting of the applicant's information and the ARC's assessment of similar applications by that entity – are uploaded to a database maintained by ASIO and searched against various intelligence holdings.

Where an applicant yields no matches with ASIO intelligence information, the check result is returned to the ARC as a simple 'negative' result, enabling the

135 This is one of the statutory functions of ASIO: *ASIO Act* (n 106) ss 17(1)(c), 37(1).

136 Ibid s 4 (definition of 'security').

137 As a result of the *Australian Security Intelligence Organisation Amendment Act 2023* (Cth) sch 1 item 7.

138 Tom Ravlic, 'ASIO Opposes Publication of its University Monitoring Activities', *The Mandarin* (online, 17 February 2023) <https://www.themandarin.com.au/212476-asio-opposes-publication-of-its-university-monitoring-activities>.

139 Australian Criminal Intelligence Commission, 'How the Service Works', *National Police Checking Service* (Web Page) <https://www.acic.gov.au/services/national-police-checking-service/find-out-more-information/how-service-works>.

rest of the grant checking process to continue. Where there is a match to ASIO holdings, this generates a 'potential match' and a referral to a workgroup within ASIO to confirm the nature of the match.[140] This enables the ASIO workgroup to not only receive a timely notification of activities by that entity in the form of a grant application, but also alerts the ARC as to potential issues that may exist and warrant referral to the DDC.

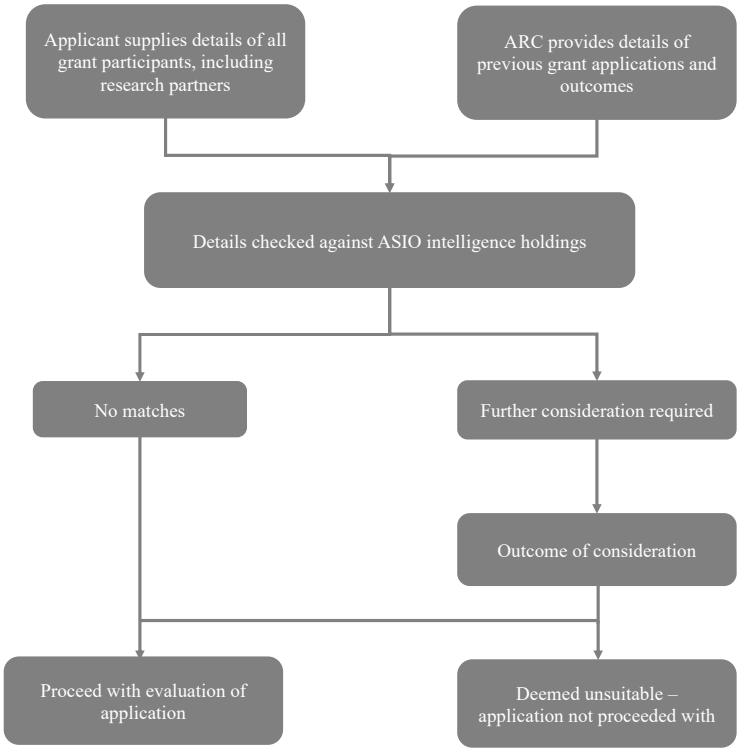

Figure 1: Proposed research security clearinghouse for grant applications

The benefits of such a system would be plentiful. Firstly, the grant applicant would need to ensure that all parties provide consent to the checking process as part of the grant application, ensuring that the ARC can meet its obligations under privacy legislation. Secondly, system access for referral of grants could be provided not only to the ARC, but also to the CSIRO and NHMRC during their grant funding and administration tasks. Thirdly, most of the system would be automated and therefore involve need for human involvement on individual referrals – only those where a 'potential match' is generated would be the subject of a formal assessment by ASIO. Fourthly, the system would not prevent the ARC from undertaking its own

140 Similar to 'potential matches' for criminal history information, which are referred to the relevant State Police forces for verification: ibid.

form of due diligence checks in addition. Fifthly, the system ensures that the ARC is not handling or receiving any classified intelligence and cannot actually access the material on which the 'potential match' is based (unless this information was supplied by ASIO as part of a formal security assessment or similar lawful release).

C The Proper Place for the Ministerial Veto

The nature of the Ministerial veto was perhaps one of the more maligned features of the *ARC Act*, in that it provided an opportunity for the Minister to refuse to fund applications which had passed all other checks and balances within the peer review process of the ARC. This was reinforced in the *ARC Review Report*, where '[e]xpert and peer review, however imperfect, has repeatedly been demonstrated to be the best system to identify talent and foster new opportunities'.[141]

However, the new amendments introduced in the *ARC Amendment Act* show huge promise in the management of research security. The Ministerial intervention now only permits the Minister to exercise their veto in respect of national security matters. For example, section 4 of the *ARC Act* has been amended to include definitions of *foreign government body*, *foreign intelligence agency*, *foreign law enforcement agency* and *foreign military body*, all of which are definitions designed to capture foreign institutions of concern which pose national security risks to the research enterprise.[142] The new section 55(1) of the *ARC Act* requires the Minister, in deciding 'whether there are reasons relevant to the security, defence or international relations of Australia' in making a funding decision, to consider:

(a) Financial support from a foreign government body (subsection (a));
(b) association with international tertiary education institutions (subsection (b));
(c) Associations with foreign governments, foreign law enforcement agencies, foreign military and intelligence agencies (subsection (c));
(d) Association with countries under sanctions from the United Nations or Australia (subsection (d));
(e) Association with entities proscribed in accordance with the *Autonomous Sanctions Act*, which deals with persons and entities of international concern (due to issues such as proliferation of weapons of mass destruction or serious human rights abuses) (subsection (e));
(f) Association with persons or entities proscribed in accordance with Part 4 of the Charter of the United Nations Act 1945 (relating to terrorism or assets relating to terrorism) (subsection (f)).

If the Minister forms the view that, 'for reasons relevant to the security, defence or international relations of Australia', the Board should not give approve a funding application made to it, the Minister must give the Board a notice in writing of that effect and the Board must comply with that notice.[143] Such notices are not legislative instruments, but must still be provided to the PJCIS as soon as

141 *ARC Review Report* (n 36) 4.
142 *ARC Act* (n 25) s 4.
143 Ibid s 47(8). Similar powers exist for refusing funding of designated research programs (s 48(6)) and ceasing payments already made or committed to under the NCGP (s 52(1)).

practicable after the decision is made, then subsequently tabled in each House of Parliament within 15 sitting days.[144]

The significance of these changes cannot be overstated. The Minister is now only permitted to exercise their veto specifically in relation to research security concerns, but those concerns may be founded upon a wide range of matters which the Minister must have regard to. Those matters themselves turn to many of the potential threats that arise under the parameters of research security, including associations or partnerships with foreign intelligence, security, law enforcement and political bodies.

The amendments contained in the *ARC Amendment Act* are of significant and substantial import for Australian universities. These amendments specifically amends the object of the Act, which will include ensuring 'support [for] research integrity [and to] promote ethical research'.[145] The ARC Board has also been restored,[146] given functions to determine the priorities for the ARC as well as to advise the Minister on research matters and assist the Minister in the performance of functions.[147] Rather than the Minister approving individual grant applications on the recommendation of the ARC, the ARC Board will now be empowered to approve grant applications per se.[148] Though the Minister has a limited ability to refuse grants to designated funding programs, any decisions (grants and refusals) must be tabled in Parliament.[149] The transparency and public scrutiny of funding matters by the ARC will go some way to repairing the trust relationship with universities, but those same universities will need to be aware of the ongoing risks, not just at the start of a research arrangement but throughout the entirety of the funding lifecycle.[150]

V CONCLUSION

The ARC has held a largely ignored role in providing Australian universities with security over the past two decades. However, the ARC's role will take increasing

144 Ibid ss 56(1)–(2).

145 *ARC Act* (n 25) s 3.

146 The previous ARC Board was abolished in 2006: Richard Grant, *The Uhrig Review and the Future of Statutory Authorities* (Research Note No 50 of 2004–05, Parliamentary Library, Parliament of Australia, 30 May 2005) <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22library%2Fprspub%2FAS6G6%22>.

147 *ARC Act* (n 25) s 9(1).

148 Ibid s 47(1).

149 Ibid s 48(8).

150 Grant Harman and Kay Harman, 'Governments and Universities as the Main Drivers of Enhanced Australian University Research Commercialisation Capability' (2004) 26(2) *Journal of Higher Education Policy and Management* 153 <https://doi.org/10.1080/1360080042000218230>; Prasada Reddy, 'The Evolving Role of Universities in Economic Development: The Case of University-Industry Linkages' in Bo Göransson and Claes Brundenius (eds), *Universities in Transition: The Changing Role and Challenges for Academic Institutions* (Springer, 2011) 25; Quan A Nguyen, Alex Maritz and Jan A Millemann, 'Entrepreneurship Imperatives in Higher Education Institutions: The Case of Australian Universities' (2022) 36(5) *Industry and Higher Education* 493 <https://doi.org/10.1177/09504222211059744>.

primacy now as the *ARC Amendment Act* has been passed by Commonwealth Parliament and in future as the functions of the Board become more commonplace. As one of the key funders of Australian research, the ARC will have to be more inwardly and outwardly resilient whilst also adopting global best practice to ensure espionage, foreign interference and intellectual property theft never become a systematic threat to Australian institutions.

One of the largest challenges to securing the university research enterprise has been the proper distinctions of responsibilities between university, government and the individual researchers. In the case of the DREAMS Lab in the Netherlands, the University of Amsterdam and the Free University of Amsterdam collaborated to create an artificial intelligence laboratory. However, they sought funding from Chinese technology company Huawei, a company well known for courting controversy. In addition to being banned from supplying 5G telecommunications technology in the US, Canada, Australia, the United Kingdom, Japan and Taiwan (amongst others),[151] allegations surfaced that Huawei technology was being used to racially profile the minority Uyghurs in China's Xinjiang province.[152] When the Huawei funding was exposed, the Dutch government claimed the universities were obligated to 'make a thorough assessment of the opportunities and the risks and to make sure that you are well-informed', and researchers responded that the Dutch government was 'unjustly confronting universities with geostrategic and security problems that are the responsibility of politics'.[153]

Australia must be careful not to fall into this trap. In the Netherlands, the DREAMS Lab controversy was just one reason for the government to move away from the co-designed regulatory process which created the National Contact Point for Knowledge Security.[154] Despite fierce opposition by the university sector, the Government is pressing ahead with a proposed screening law which would obligate universities to check the backgrounds of every foreign researcher prior to their being given a Dutch residency permit.[155] By foregoing cooperative design at the institutional level, the Netherlands government now risks a 'rather uncoordinated policy response, including risks of overregulation, unalignment, and blind spots'.[156] The stage is clearly set for funding bodies to:

> …develop guidelines that consider the increasingly multipolar research landscape amid geopolitical tensions. The research sector's inability to handle matters related

151 Noah Berman, Lindsay Maizland and Andrew Chatzky, 'Is China's Huawei a Threat to US National Security?', *Council on Foreign Relations* (Backgrounder, 8 February 2023) <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security>.

152 David Snetselaar, 'DREAMS Lab: Assembling Knowledge Security in Sino-Dutch Research Collaborations' (2023) 32(2) *European Security* 233, 235 <https://doi.org/10.1080/09662839.2022.2127317>.

153 Ibid 245.

154 'National Contact Point for Knowledge Security', *Netherlands Enterprise Agency* (Web Page, 12 January 2022) <https://english.rvo.nl/topics/national-contact-point-knowledge-security>.

155 *Wet voor het Toetsingskader ongewenste kennis en technologieoverdracht* [screening legislation for undesirable knowledge and technology transfer].

156 Chris Eveleens, *Policy Responses Strengthening Knowledge Security: A Comparative Study of Austria and the Netherlands* (Research Paper, Advisory Council for Science, Technology and Innovation, December 2023) 11.

> to data security, multiple affiliations, or ethics dumping can mean that national political forces are likely to use additional compliance.[157]

There will undoubtedly need to be further research into the impacts of increased national security scrutiny on NCGP funding. At least one academic whom the author has spoken to about this kind of research anecdotally commented 'well that's all well and good, but China is where all the money is'. Efforts to prevent or block cooperations with certain entities may risk future innovations, foreclose opportunities or even rise to the level of political or diplomatic repercussions.[158] The imposition of stricter controls may also result in the 'cockroach phenomenon',[159] driving even the most well-intentioned researchers into seeking funding from less reputable sources. One study in the US showed that even temporary shocks to federal funding drove universities to prioritise sources of private funding.[160]

There is also perhaps a more fundamental need to re-examine the grant funding processes under the NCGP. The *ARC Review Report* was replete with examples of concerns around 'poor prospects of securing ARC funding for early career researchers', the length of time and resources invested in ultimately unsuccessful grant applications distracting from core business, and the risks of 'privileging style and particular kinds of research outcomes'.[161] Humanities subjects were particularly hard hit, not just by Ministerial vetos[162] but also by the way researcher metrics are assessed in the grant process.[163] Finally, the emergence of new technologies (like ChatGPT) has also raised suggestions that if a computer can write a successful grant application, then the criteria for success must be entirely arbitrary.[164] The future of the ARC will depend on its ability to manage these challenges whilst also looking to protect that most fundamental of Australian university outputs – research in the national public interest.

---

157 Tommy Shih, Andrew Chubb and Diarmuid Cooney-O'Donoghue, 'Scientific Collaboration Amid Geopolitical Tensions: A Comparison of Sweden and Australia' (2024) 87 *Higher Education* 1339, 1353 <https://doi.org/10.1007/s10734-023-01066-0>.

158 See eg, Australia's calls for an independent inquiry into the origins of COVID-19 were met with trade tariffs by China on wine, beef and barley: Jeffrey Wilson, 'Australia Shows the World What Decoupling from China Looks Like', *Foreign Policy* (online, 9 November 2021) <https://foreignpolicy.com/2021/11/09/australia-china-decoupling-trade-sanctions-coronavirus-geopolitics>.

159 So-called because of the behaviour of cockroaches which scurry for hiding places when the lights are switched on: Ian Hosein, Prodromos Tsiavos and Edgar A Whitley, 'Regulating Architecture and Architectures of Regulation: Contributions from Information Systems' (2003) 17(1) *International Review of Law, Computers and Technology* 85, 90 <https://doi.org/10.1080/1360086032000063147>.

160 Tania Babina et al, 'Cutting the Innovation Engine: How Federal Funding Shocks Affect University Patenting, Entrepreneurship, and Publications' (2023) 138(2) *Quarterly Journal of Economics* 895 <https://doi.org/10.1093/qje/qjac046>.

161 *ARC Review Report* (n 36) 21, 35, 57 respectively.

162 Ibid 29.

163 Ibid 57. Ironically, humanities research is one of the fields as critically important in developing and formulating research security principles: Brian Lennon, 'The Digital Humanities and National Security' (2014) 25(1) *Differences* 132 <https://doi.org/10.1215/10407391-2420027>; Claudia Aradau, Tobias Blanke and Ibtehal Hussain, 'Making Data Visualizations, Contesting Security: Digital Humanities Meet International Relations' (2023) 3(4) *Global Studies Quarterly* 1 <https://doi.org/10.1093/isagsq/ksad061>.

164 Juan Manuel Parrilla, 'ChatGPT Use Shows that the Grant-Application System is Broken' (2023) 623 *Nature* 443 <https://doi.org/10.1038/d41586-023-03238-5>.