Submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade

Inquiry into the review of the operation of the amendments made by the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021

Outline and Summary

Thank you for the opportunity to make a submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade (the Committee) on their review of the *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021* (Cth) (Magnitsky Act). The purpose of the Magnitsky Act was to amend Australia's autonomous sanctions regime to provide the Minister for Foreign Affairs (with the agreement of the Attorney-General) with the ability to proscribe persons or entities as subject to targeted financial sanctions and travel bans on either country-specific and/or thematic bases.

This submission has been prepared by myself in my capacity as a Senior Lecturer in the Law Discipline at Southern Cross University. However, the views expressed below are entirely my own and may not be representative of the Law Discipline, Southern Cross University or any other government, organisation or agency. Further, certain organizations are identified in this submission by name. Their inclusion in this submission is not, and should not be taken to be, any imputation or suggestion of guilt or wrongdoing beyond that reasonably conveyed by reference to third-party source material.

This submission will touch only on certain matters within the Magnitsky Act, and should not be viewed as endorsement or opposition of any other provisions in the Magnitsky Act.

Australia's Sanctions Regime generally

The Explanatory Memorandum[1] makes clear that the application of sanctions under Australian law is two-pronged: either multi-laterally (by enforcement of 'international obligations arising from United Nations Security Council (UNSC) decisions') or unilaterally (being "autonomous" sanctions, those 'punitive measures, not involving the use of armed force, which a government imposes as a matter of foreign policy').[2] Indeed, the Explanatory Memorandum explains that the policy purpose of such autonomous sanctions is to 'limit the adverse consequences of the situation of international concern and to influence and penalise those responsible for giving rise to the situations while minimising, to the extent possible, the impact on the general population'.[3]

The Committee's earlier review sets out the widely accepted two-step process for issuing autonomous sanctions under Australian law:

> First the Minister must advise the Governor-General to amend the Regulations to identify the targeted country and the activities for which a person or entity could be designated. The Minister must then make a second instrument to designate a specific person or entity, pursuant to regulation 6(1). The Minister must be satisfied that the person or entity meets a range of criteria set out in Regulation 6.[4]

---

[1] Explanatory Memorandum to the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Bill 2021.
[2] Ibid, 1.
[3] Ibid.
[4] Joint Standing Committee on Foreign Affairs, Defence and Trade, *Inquiry into Criminality, Corruption and Impunity: Should Australia Join the Global Magnitsky Movement?* (Final report, 7 December 2020) ("Committee Review Report") [2.24].

That process has not been significantly amended by the Magnitsky Act (however, the Foreign Minister may choose to consult such Ministers as he or she deems appropriate prior to the Governor-General amending the Regulations). The grounds for issuing thematic sanctions has now also been enacted under Regulation 6A, setting out the matters which the Minister must be satisfied of prior to making a designation or declaration under the Act. On that basis, the Minister may:

- **Designate** a person or entity if the Minister is satisfied that they are contributing to the proliferation of weapons of mass destruction (WMD), significant cyber incidents, serious violations or serious abuses of human rights, and/or serious corruption; and/or
- **Declare** that a designated person or entity is subject to a given sanction.

Both before and after the enactment of the Magnitsky Act, the Minister for Foreign Affairs (the Minister) has caused the Department of Foreign Affairs and Trade (DFAT) to maintain a list of current autonomous and UNSC sanctions, known as the "Consolidated List". That list is freely available to members of the public to conduct searches on persons or entities that are subject to sanctions from time to time.[5]

A division of DFAT known as the Australian Sanctions Office (ASO) is the regulator for Australia's sanctions regime, together with the Australian Federal Police (for the purposes of investigating and prosecuting any breaches of sanctions law).[6]

The previous Reviews of the *Autonomous Sanctions Act 2011* (Cth)

The Magnitsky Act was a recognition of the Government's response of 5 August 2021 following the Committee's inquiry (conducted by its Human Rights Sub-committee) into the use of sanctions to target human rights abuses entitled *Criminality, corruption and impunity: Should Australia join the Global Magnitsky movement?*. That report recommended adoption of a regime enabling so-called "Magnitsky" sanctions, so named because of:

> …Mr Sergei Magnitsky, a Russian tax lawyer who worked for Hermitage Capital Management, owned by Mr Bill Browder, an American financier… uncovered a massive fraud committed by Russian government officials that involved the theft of US $230 million of state taxes. Mr Magnitsky testified against the officials involved and was subsequently arrested by them, imprisoned, systematically tortured and killed in Russian police custody on November 16, 2009… the Russian authorities covered up his murder, exonerated all the officials involved … [and] put Sergei Magnitsky on trial three years after they killed him.[7]

The Committee's report of the inquiry was fuelled in large part by observance of the US *Sergei Magnitsky Accountability Act of 2012*, as well as the passage of the US *Global Magnitsky Human Rights Accountability Act of 2017* and US Presidential Executive Order 13818 'Blocking the Property of Persons Involved in Serious Human Rights or Corruption'.

The previous Report into the Magnitsky Act by the Committee recommended *inter alia* among its 33 recommendations that new legislation – based on a draft prepared by well-known human rights

[5] Department of Foreign Affairs and Trade, *Consolidated List* (website, 9 December 2024) <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>.
[6] Which includes criminal penalties of up to ten years in prison and/or a fine (the greater of $687,500 or three times the value of the transaction) for individuals, and fines for corporations (the greater of $2.75 mil or three times the value of the transaction).
[7] Mr William Browder, Submission No 4 to the Committee, *Inquiry into Criminality, Corruption and Impunity: Should Australia Join the Global Magnitsky Movement?*, 1; cited in Committee Review Report, [1.11].

lawyer Mr Geoffrey Robertson AO KC – ought be adopted by Parliament to address the issue of thematic sanctions for human rights abuses and corruption.[8]

The response, tabled on 5 August 2021, confirmed the Government's in-principle support for amendment of the sanctions regime to incorporate human rights and corruption as grounds for the imposition of sanctions. However, some of the more contentious parts of the Committee's report – including the establishment of an independent advisory body to review and recommend sanction targets to the Minister and a "right of reply" for proposed sanction targets – were outright rejected.[9]

Following the Committee's review, in 2023 DFAT conducted a statutory review (DFAT Review) of Australia's autonomous sanctions framework ahead of the-then sunsetting of the *Autonomous Sanctions Regulations 2011* (Cth) on 1 April 2024. The purpose of the DFAT Review was to:

> …examine how the autonomous sanctions framework could better support the government's foreign policy objectives. In doing so, it will consider whether the Regulations and associated instruments remain fit for purpose and will seek to identify administrative and regulatory efficiencies for government and the public, with a view to ensuring robust sanctions compliance.[10]

The DFAT Review received 27 submissions and published a final report on 30 October 2023.[11] That final report identified seven key issues for consideration in adopting the Magnitsky reforms:

- Streamlining the legal framework for autonomous sanctions
- Reviewing the scope of sanctions measures
- Improving the issuance of permits for persons to deal with sanctioned entities
- Including a humanitarian exemption to autonomous sanctions
- Sanctions offences and enforcement, including the possibility of introducing civil penalties
- Creating a review mechanism for sanctions designations and declarations
- Reviewing the regulatory functions of the ASO.

Of those seven key issues, none have seen substantial public progress (though it is possible that such recommendations have been considered by DFAT internally). Importantly, the DFAT Review identified three broad themes that will be of importance in the Committee's review of the Magnitsky Act: the scope of sanctions measures, the review pathway for imposed sanctions, and the regulatory functions of the ASO.

Recommendation 1: That the Committee consider what (if any) progress has been made by DFAT in progressing the seven key issues identified in the previous Review and make such recommendations to Government on dealing with those issues as it considers appropriate.

[8] Committee Review Report, xxi-xxiv.
[9] Australian Government, *Response to the Joint Standing Committee on Foreign Affairs, Defence and Trade Human Rights Sub-Committee report: Inquiry into Criminality, Corruption and Impunity: Should Australia Join the Global Magnitsky Movement?* (5 August 2021) ("Australian Government Response") 8-9 and 10-11.
[10] Department of Foreign Affairs and Trade, *Terms of Reference – Review of the legal framework for autonomous sanctions* (30 January 2023) <https://www.dfat.gov.au/news/news/review-australias-autonomous-sanctions-framework-issues-paper>.
[11] Department of Foreign Affairs and Trade, *Report on the review of Australia's sanction laws* (30 October 2023) <https://www.dfat.gov.au/international-relations/security/sanctions/reform-australias-sanctions-laws>.

Comparable sanctions regimes internationally

A helpful analysis of international sanctions regimes prior to the adoption of the Magnitsky Act in Australia is available in the Committee's review report.[12]

Like Australia, the United States International Trade Administration (part of the US Department of Commerce) publishes a Consolidated List, which it synthesises using multiple lists from across the US Government.[13] However, the genesis of the lists available on the US Consolidated List are markedly different to Australia. For example, the Bureau of Industry and Security – also part of the US Department of Commerce with responsibility for administering the Export Administration Regulations (EAR)[14] – maintains four separate lists:

- **Denied Persons List**: A list of individuals and entities that have been denied export privileges.
- **Entity List:** The Entity List identifies foreign parties that are prohibited from receiving some or all items subject to the EAR unless the exporter secures a license.
- **Unverified List:** A list of parties whose bona fides BIS has been unable to verify, and to whom exports are not permitted without a verification statement acceptable to BIS.
- **Military End User List:** The Military End User List contains parties that have been determined by the US Government to be 'military end users'. Exporters require a licence to export military equipment or technologies listed in Supplement No. 2 of Part 744 of the EAR to these entities.

Of relevance here is the "Entity List", which BIS defines as containing a list of individuals and entities that:

> …present a greater risk of diversion to weapons of mass destruction (WMD) programs, terrorism, or other activities contrary to U.S. national security and/or foreign policy interests. By publicly listing such parties, the Entity List is an important tool to prevent unauthorized trade in items subject to the EAR. BIS can add to the Entity List a foreign party, such as an individual, business, research institution, or government organization, for engaging in activities contrary to U.S. national security and/or foreign policy interests.[15]

Items included on the EAR may not be exported, reexported, or transferred (in-country) to any person or entity on the Entity List without a licence.[16]

Similar "end user" lists have also been adopted by Canada,[17] Japan,[18] and the European Union.[19]

---

[12] Committee Review Report, [3.45]-[3.69].
[13] International Trade Administration, *Consolidated List Search* (website, 2024) <https://www.trade.gov/data-visualization/csl-search>.
[14] 15 CFR 730-774.
[15] Bureau of Industry and Security, Lists of Parties of Concern (website, 2024) <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern>.
[16] 15 CFR §744.16 and Supplement No. 4 to Part 744.
[17] Innovation, Science and Economic Development Canada, *Named Research Organisations* (website, 4 January 2024) <https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1082-named-research-organizations-list-09Jan2024.pdf>.
[18] Ministry of Trade and Investment (METI), *Review of the End User List* (website, 4 November 2022) <https://www.meti.go.jp/english/press/2022/1104_002.html>.
[19] Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *Consolidated list of persons, groups and entities subject to EU financial sanctions* (website, 22 October 2024) <https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en>.

The United Kingdom (UK) also permits the imposition of sanctions under the *Sanctions and Anti-Money Laundering Act 2018* (UK) ("SAMLA"). Once declared, a person or entity may be subject to travel bans, asset freezes, limits on immigration or trade, or the entry to the UK of certain aircraft or vessels in the same way that sanctions can be applied under Australian law.[20]

However, the scope and applicability of UK sanctions law is far broader than that in Australia. A helpful comparison between the scope of sanctions available to the Australian and UK Ministers is shown below in Table 1.

Australia's Autonomous Sanctions Act 2011 (Cth), s 3(3)	*Sanctions and Money Laundering Act 2018* (UK), s 1(2)
…autonomous sanctions may address one or more of the following: (a) the proliferation of weapons of mass destruction; (b) threats to international peace and security; (c) malicious cyber activity; (d) serious violations or serious abuses of human rights; (e) activities undermining good governance or the rule of law, including serious corruption; (f) serious violations of international humanitarian law.	A purpose is within this subsection if the appropriate Minister making the regulations considers that carrying out that purpose would: (a) further the prevention of terrorism, in the United Kingdom or elsewhere, (b) be in the interests of national security, (c) be in the interests of international peace and security, (d) further a foreign policy objective of the government of the United Kingdom, (e) promote the resolution of armed conflicts or the protection of civilians in conflict zones, (f) provide accountability for or be a deterrent to gross violations of human rights, or otherwise promote— (i) compliance with international human rights law, or (ii) respect for human rights, (g) promote compliance with international humanitarian law, (h) contribute to multilateral efforts to prevent the spread and use of weapons and materials of mass destruction, or (i) promote respect for democracy, the rule of law and good governance.

Table 1: Comparison of the scope of autonomous sanctions under Australian and UK law

Table 1 demonstrates that the UK sanctions law is more permissive and broader in scope. For example, the UK responsible Minister may issue sanctions against a person or entity 'in the interests of national security', to 'further a foreign policy objective of the government [of the United Kingdom]', 'promote the resolution of armed conflicts or the protection of civilians in conflict zones', and/or 'promote respect for democracy, the rule of law and good governance'.

These provisions will be examined in more detail later in this submission.

The emergence of research security

Since the Committee's last review in 2021, both Defence and national security environments confronting Australia have changed significantly. Australia has entered into the AUKUS Agreement to

[20] Ibid, ss 3-8.

fast-track the delivery of certain cutting-edge capabilities, including nuclear powered submarines, hypersonics, undersea autonomous vehicles, robotics and quantum computers. The receipt of this technology will largely be facilitated by universities, where ongoing research to further these technologies will also occur. Thus, the continuation of this arrangement will likely require a significant security uplift for peculiar segments of university research being conducted in the national interest.

At the same time, national security threats to our higher education institutions are not academic: they are happening now. Universities have been told to "harden" their posture against foreign interference and espionage,[21] but have been given limited information on how best to do so.[22] Our students and academics are being threatened in Australia and abroad, by agents posing as debt collectors[23] and anti-corruption officers.[24] Our allies are also experiencing these same threats on their campuses and in their classrooms.[25] Yet, just two years after the Parliamentary Joint Committee on Intelligence and Security (PJCIS) handed down its report on national security risks in HEIs,[26] less than half of the recommendations of the PJCIS were supported, and almost none have been fully implemented.[27]

To combat these threats, global universities are recognising the importance of adopting "research security" programs. Research security is a term predominantly in use in the American and Canadian research ecosystems, both of which are more matured than Australia to refer to '*the ability to identify possible risks to your work through unwanted access, interference, or theft and the measures that minimize these risks and protect the inputs, processes, and products that are part of scientific research and discovery.*'[28]

My submission places the ideas of research security at the centre of a call to refocus some elements of Australia's sanctions law to protecting Australia's research ecosystem. It is without question an incredibly important industry to Australia, not only economically, socially and culturally, but also for the future of our diplomacy, security and defence strategies in both regional and global contexts. The

---

[21] Joseph Brookes, 'Universities told to "harden" against foreign interference threat', *Innovation Australia* (website, 28 March 2022) <https://www.innovationaus.com/universities-told-to-harden-against-foreign-interference-threat/>.
[22] 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/>.
[23] Stella Yifan Xie, 'When China's Aggressive Debt Collectors Come Knocking: "You Committed a Sin"', *The Wall Street Journal* (online, 15 June 2020) <https://www.wsj.com/articles/when-chinas-aggressive-debt-collectors-come-knocking-you-committed-a-sin-11592227095>.
[24] Mark Walden, 'Operation Fox Hunt and China's international efforts to force "fugitives" back', *ABC News* (online, 19 January 2022) <https://www.abc.net.au/news/2022-01-19/china-operations-to-force-fugitives-back/100747234>.
[25] Nidhi Subbaraman, 'Universities Forge Ties with FBI Amid Foreign Influence Crackdown' (2020) 579 *Nature* 331; Charlie Parker, 'Iranian regime exploits deals with UK unis to help develop weapons', *The Australian* (online, 31 July 2023) < https://www.theaustralian.com.au/world/the-times/iranian-regime-exploits-deals-with-uk-unis-to-help-develop-weapons/news-story/10e0c681ae93959fe409c54577a201e3>.
[26] Commonwealth Parliament, *Inquiry into national security risks affecting the Australian higher education and research sector* (Final Report, March 2022) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Report> ("the PJCIS Report").
[27] 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, 14 February 2023) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Government_Response>.
[28] Government of Canada, *Why Safeguard your Research?* (website, 31 March 2023) <https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/why-safeguard-your-research >.

alternative – a university sector which ignores or minimises the threat posed – has the potential to threaten our international diplomatic and defence ties, our regional standing, and the achievement of Australia's medium- and long-term strategic objectives. That situation cannot be allowed to prevail.

Consider the position of Australia compared to other developed economies:

- In the United States, research security is a fundamental part of the US research enterprise, and which embeds counter-foreign interference and counter-espionage systems in all national funding applications.[29] The US National Science Foundation has also just committed US$67 million to establish a Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) centre between government and universities.[30]
- The Netherlands Government has established the *National Contact Point for Knowledge Security*, an online clearing house for collaboration across ministries and the university sector 'with questions about opportunities, risks and practical matters concerning international cooperation'.[31] The Contact Point provides deidentified case studies of espionage and intellectual property theft, legal frameworks for export control and foreign interference, and a direct helpline into Government for researchers.
- In Canada, the Canadian Security Intelligence Service (CSIS) plays a key role in mitigating national security threats to HEIs. In particular, the CSIS provides a "Safeguarding your Research" checklist, as well as links to a centralised repository of tools to assist HEIs in managing their national security risk.[32] Key amongst these are the *Named Research Organisations* and *Policy on Sensitive Technology Research and Affiliations of Concern*, which are mandatory for all Federally funded research grants and considered "strongly recommended" for all other forms of funding.[33]
- Across the broader EU, the European Commission has formulated guidelines for HEIs to enhance their 'values, governance, partnerships and cybersecurity' in the face of foreign interference in research and innovation, with specific focus on HEIs.[34] In May 2024, the European Commission accepted a recommendation to enhance the research security of the EU, calling on all Member States to take steps to address the 'undesirable transfer of knowledge, foreign interference, and ethical or integrity violations'.[35]

---

[29] National Science Foundation, *Research Security at the National Science Foundation* (website, 2022) <https://new.nsf.gov/research-security >.
[30] 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>.
[31] Government of the Netherlands, *Contact Point for Knowledge Security* (website, 2022) <https://english.loketkennisveiligheid.nl/ >.
[32] Government of Canada, *Safeguarding Your Research* (website, 2022) <https://science.gc.ca/site/science/en/safeguarding-your-research>.
[33] Innovation, Science and Economic Development Canada, *Policy on Sensitive Technology Research and Affiliations of Concern* (January 2024) <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern>.
[34] European Commission, *Tackling R&I foreign interference* (Working document, Publications Office of the European Union, 2022) <https://data.europa.eu/doi/10.2777/513746>.
[35] Council of the EU, *Council adopts a recommendation to enhance research security* (media release, 23 May 2024) <https://www.consilium.europa.eu/en/press/press-releases/2024/05/23/council-adopts-a-recommendation-to-enhance-research-security/>.

Australia's own approach to research or knowledge security is somewhat lamentable. The University Foreign Interference Taskforce (UFIT) Guidelines,[36] originally produced in 2019 and refreshed in 2021, do not adequately address several areas of risk. Further, as the PJCIS observed in 2021, the UFIT Guidelines do not address all national security risks to HEIs and are not benchmarked across the sector, meaning responses are fragmented and incomplete across numerous institutions.[37]

The UFIT Guidelines are also largely devoid of specific content, being more "aspirational" in nature, leaving individual institutions in Australia to implement their own versions of compliance with it. These Guidelines vaguely recommends that universities and higher education institutions conduct due diligence and risk assessments 'on partners and personnel' as well as 'the potential of technology and/or research'. Unfortunately, neither universities nor individual researchers have the resources or expertise to properly vet those partners or personnel for risks to national security.

Governmental organisations fare no differently. The Australian Research Council (ARC) – the statutory body of the Commonwealth which administers the $800 million a year in funding under the National Competitive Grants Program (NCGP) – has almost no resources on dealing with research security.[38] The ARC does not publish information about grants or projects (even on a deidentified basis) which are refused for national security reasons, or which may attract particular risks. Other Commonwealth funding bodies (such as the National Health and Medical Research Council) do not appear to have any public resources on research security at all.

The Magnitsky Act carries within it the capability for the Minister to more comprehensively address research security than has previously been the case. What is now needed is limited reform of Australian sanctions law and a political willingness to use it for this purpose.

Recommendation 2: The Committee should consider the emerging debate about research security threats occurring around the world and note the use of sanctions law by our allies to address specific threats to their national research enterprises.

Research security and sanctions law

In 2023, I provided a submission to the Panel of the Australian Universities Accord. In that submission I suggested that the government should consider enacting legislation to permit the listing of organisations or entities which pose national security threats to Australian HEIs from either research or teaching perspectives. Such listing should include (as a minimum):

- "Black-listing" – describing entities whose behaviours, public statements or connections pose unacceptable levels of risk to Australia's security, defence, international relations or foreign policy objectives. Collaborations with "black-listed" entities, irrespective of country of origin, should be banned.
- "Grey-listing" – describing entities whose academic or other credentials cannot be suitably verified to the satisfaction of the Australian government. Collaborations with "grey-listed"

[36] Department of Education, *Guidelines to Counter Foreign Interference in the Australian University Sector* (17 November 2021) <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector >.
[37] The PJCIS Report, n 19, 136-137.
[38] However, they have published their Countering Foreign Interference Strategy as at December 2023: Australian Research Council, *ARC Countering Foreign Interference Framework* (website, December 2023) <https://www.arc.gov.au/sites/default/files/2023-12/ARC%20Countering%20Foreign%20Interference%20Framework.pdf>.

entities may be permissible if a HEI has undertaken sufficient due diligence and enacted robust risk control measures in relation to that collaboration.

- "Red-listing" – describing entities whose connections with military personnel, organisations or facilities pose an unacceptable risk that information, knowledge or technology shared with such entities may be diverted to military "end-use".[39]

My submission should not be viewed as endorsement for any form of ban on international students, doctoral candidates, or academics from one specific nationality, merely because of that nationality. Such ban are a highly radical, controversial and potentially unlawful approach to the treatment of national security risk on the following grounds:

1. Such "bans" may result in reciprocal limitations or sanctions being imposed by the offended country, and which may go beyond the academic and potentially result in economic, diplomatic, or political costs which outweigh the possible benefit;[40]
2. It would be extremely difficult to identify what areas of research, or what sub-specialities within a field, could be captured as "high-risk". The difficulty is analogous to "dual-use" technologies, which are civilian technologies which may also be used or repurposed for military, security, or intelligence purposes;[41] and
3. A ban on students from a particular country, even on grounds of national security, might be considered a form of unlawful racial discrimination,[42] as well as violating Australia's various international human rights obligations.[43]

Instead, I would propose that the Committee consider making recommendations to the Australian Government that they consider a reform program of Australian sanctions law designed to bolster specific aspects of Australian research security. My broad submission on this point is that:

The Magnitsky reforms could provide the Minister with power under Australian sanctions law to protect the Australian research ecosystem.

I note that the Magnitsky reforms were grounded in a focus on countering serious human rights, corruption, and breaches of international law and legal rights. Yet the evidence is overwhelming that sanctions law could be both capable of dealing with the highest risk threats to Australian research security and providing an extremely useful toolkit for the Minister to secure Australia's research ecosystem from harm or interference.

---

[39] *Customs Act 1901* (Cth), s 112BA.

[40] For an example, see reports of the directive in 2021 banning Chinese education agents from sending students to Australian universities: Julie Hare, 'Chinese students told not to study in Australia', *Australian Financial Review* (online, 25 February 2021) <https://www.afr.com/policy/health-and-education/chinese-students-told-not-to-study-in-australia-20210225-p575t1>.

[41] Jan Famfollet, *Protection of Strategic and Dual-Use Technologies* (Report, 2022) <https://europeanvalues.cz/en/protection-of-strategic-and-dual-use-technologies/>.

[42] *Racial Discrimination Act 1975* (Cth), s 9(1): It is unlawful for a person to do any act involving a distinction, **exclusion**, restriction or preference based on race, colour, descent or **national or ethnic origin** which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of any human right or fundamental freedom in the political, economic, social, cultural or any other field of public life (emphasis added).

[43] See for example the issues in banning the hijab in Ibrahim Abraham, 'Hijab in an age of fear: Security, secularism, and human rights' (2006) 19(2) *Australian Religion Studies Review* 169.

Use of the existing sanctions law for research security

As a specific point of reference, DFAT already publishes information for universities on the application of Australian sanctions law to their operations.[44] Advice to Australian universities on sanctions is equally aspirational, merely suggesting that they:

- familiarise themselves with all information provided on the ASO website;
- subscribe to ASO's email list to receive updates on Australian sanctions law;
- follow the *What You Need To Do* checklist;
- ensure they undertake the due diligence necessary to ensure compliance with Australian sanctions law; and
- develop a risk management strategy, verified by their own legal advice.

However, this advice does little to assist universities if the Minister has not designated or declared an entity that could pose potential grave research security risks to the Australian research ecosystem. That said, it is entirely possible (though clearly not common) for the existing scheme of Magnitsky sanctions to be applied to potential research partners outside Australia that pose risks to Australian foreign policy.

One such example involves Tsinghua University in the People's Republic of China (PRC), which has not only engaged in 'strategic cooperation' with the Chinese Academy of Engineering Physics (the entity responsible for the development of China's nuclear weaponry) but also houses infrastructure allegedly linked to cyber-attacks against the Tibetan community as well as companies and government agencies in Alaska, Kenya, Brazil, and Mongolia.[45] At the time of writing this submission, there are approximately 65 agreements between Tsinghua University and Australian entities contributing to research in this country.[46]

Given that information, Tsinghua University could be the subject of a thematic sanction if the Governor-General were to make Regulations applying to research security, and the Minister were to designate Tsinghua under those Regulations, either because of:

a.) Their 'contributing to the proliferation of weapons of mass destruction',[47] being nuclear weapons or technologies designed or developed by the PRC; or
b.) Having permitted their infrastructure to be used for cyber-attacks as 'otherwise been complicit in causing, or in attempting to cause, a significant cyber incident'.[48]

The application of Magnitsky sanctions to possible foreign research partners is certainly not ideal, lacking any specific legislative criteria in the Act or Regulations which would direct the Minister towards matters to be considered. A similar criticism was raised in the Committee's earlier inquiry by the Law Council of Australia with respect to human rights violations, with the Law Council indicating that 'although there is room within the existing autonomous sanction framework to target human

[44] Department of Foreign Affairs and Trade, Factsheet: General Guide for Universities (website, 2024) <https://www.dfat.gov.au/international-relations/factsheet-general-guide-universities>.
[45] Brendan Walker-Munro, Ruby Ioannou, David Mount, *Are we training potential adversaries? Australian universities and national security challenges to education* (Report, October 2023), <https://espace.library.uq.edu.au/view/UQ:af6347b>.
[46] Department of Foreign Affairs and Trade, *Public Register of Foreign Arrangements* (website, 2024) <https://www.foreignarrangements.gov.au/public-register>.
[47] *Autonomous Sanctions Regulations 2011* (Cth), r 6A(1)(a).
[48] Ibid, r 6A(2)(a)(iii).

rights violations, in practice this has rarely occurred, and the current Act and Regulations lack express criteria directed at this objective' (emphasis added).[49]

The result is a system of sanctions law whereby Australian universities have, and will, continue to cooperate with entities and/or in ways that may not be fully compatible with Australian foreign policy. Consider for example the case of Sharif University of Technology in Iran. For many years, Sharif University of Technology has been the subject to autonomous sanctions in the UK and elsewhere[50] because of provision of support for, and association with, the conduct of the government of Iran's nuclear proliferation activities.[51]

Despite that declaration, at the time of writing this submission there are four Australian universities with declared associations with the Sharif University of Technology.

I strongly recommend the Committee should consider whether the Australian Government should amend the existing sanctions regime to better deal with potential research partners that pose grave foreign policy risks to Australia.

Recommendation 3: The Committee should recommend that the Government amend Regulation 6A of the *Autonomous Sanctions Regulations 2011* (Cth) to specifically express criteria that would enable the Foreign Minister to consider thematic sanctions against high-risk foreign entities that pose research security threats.

Scope of sanctions

Unfortunately, the application of Magnitsky sanctions to potential foreign research partners is limited by the grounds upon which Regulations may be made and designations may occur. Only universities or other foreign entities that meet the criteria in regulation 6A may be the subject of a designation. As a matter of comparison, section 1(1) of UK's SAMLA permits the Foreign Secretary, Secretary of State or the Minister of the Treasury (as the responsible Minister) to make sanctions regulations, where the Minister is satisfied that the sanction would 'be in the interests of national security',[52] 'further a foreign policy objective of the government of the United Kingdom'[53] or 'promote respect for democracy, the rule of law and good governance'.[54]

There would be significant utility being able to issue autonomous sanctions under the same grounds as those in UK law, being grounds which are not otherwise covered by existing Australian sanctions law.

Consider the example of Beihang University in the PRC. Beihang University is considered one of the 'Seven Sons of National Defence', and specialises in research on rockets, missile and stealth aircraft

[49] Ms Pauline Wright, President, Law Council of Australia, *Committee Hansard*, Canberra, 15 June 2020, 7; cited in Committee Review Report, [2.49].
[50] At the time of writing, Canada and the EU have both sanctioned Sharif University: OpenSanctions, *Sharif University of Technology* (website, 2024) <https://www.opensanctions.org/entities/NK-nxBVUwhmE8JFVPkiVzKVaS/>.
[51] *Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019* (UK).
[52] SAMLA s 1(2)(b).
[53] Ibid s 1(2)(d).
[54] Ibid s 1(2)(i). Section 3(3) of the *Autonomous Sanctions Act 2011* (Cth) does allow for sanctions related to 'activities undermining good governance or the rule of law', regulation 6A only focuses on 'serious corruption'.

technology.[55] Beihang University has also been added to the "end user" lists of both the US and Japan for their close ties to the military and defence apparatus of the PRC. However, these matters alone are not sufficient for Beihang to be considered for potential sanction under Australia's autonomous sanctions regime, as that entity does not meet any of the criteria established by either the Act or Regulations.

This case is highly relevant because of the appeal of Xiaolong Zhu in the Federal Circuit and Family Court of Australia earlier this year.[56] Zhu's student visa to study a PhD in Australia – involving drone navigation in GPS-denied environments – was refused after the Foreign Minister declared Zhu to be a person 'whose presence in Australia may be directly or indirectly associated with the proliferation of weapons of mass destruction' under the *Migration Regulations 1994* (Cth). That determination was not a sanction *per se* and had no practical implications for Beihang University more broadly. Indeed, at the time of writing this submission, there are currently 17 agreements between Beihang University and other Australian entities.

It seems antithetical to the good execution of Australian foreign policy that an individual might be deemed 'directly or indirectly associated' with the proliferation of WMD premised on a previous association with Beihang University, yet that same university has not been the subject of designation for contribution to WMD (or indeed on any other ground). In any event, there are clear grounds that might warrant the sanctioning of Beihang University – and others like it – if the Australian sanctions regime were more permissive of grounds to designate entities. If Australia had a permissible ground that imposing a sanction would 'be in the interests of national security' as in UK legislation,[57] the situation might have been vastly different.

Recommendation 4: The Committee should recommend that the Government reform section 3(3) of the *Autonomous Sanctions Act 2011* (Cth) to align fully with the grounds for issue of "thematic" sanctions provided by section 1(2) of the United Kingdom's *Sanctions and Money Laundering Act 2018* (UK).

Ancillary effects of designations

Of course, the Minister's designation of a person or entity can still achieve ancillary effects. Imposition of a travel ban under the various permutations of Regulation 6A has ancillary effects on visa applications and visas held by a natural person who is the subject of such a ban. For example, a person subject to such a travel ban sanction enlivens cancellation of existing visas and refusal of future applications under the *Migration Regulations 1994* (Cth).[58] The consideration of those provisions by the Home Affairs Minister following any form of determination by the Foreign Minister is not an incompatible exercise of discretionary power and is not otherwise unreasonable.[59]

[55] Australian Strategic Policy Institute, *China Defence Universities Tracker: Beihang University* (website, 2024) <https://unitracker.aspi.org.au/universities/beihang-university/>.
[56] *Zhu v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2024] FedCFamC2G 411.
[57] i.e., SAMLA s 1(2)(b).
[58] *Migration Regulations 1994* (Cth), r 2.43(aa)(i) and Sch 4, PIC 4003.
[59] *Zhu v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2024] FedCFamC2G 411.

Further, it is prohibited[60] (without a permit) to allow the use of or dealing with assets[61] owned or controlled by a designated person or entity, and/or making any kind of asset available, directly or indirectly, to a designated person or entity. It is accepted that the Committee was correct when, in their earlier review, they said:

> The aim of these sanctions is primarily to act as a deterrent – by reducing the opportunity to enjoy 'ill-gotten gains' with impunity. Sanctions limit the ability for human rights abusers or those benefitting from corruption to enjoy the profits or proceeds internationally, by limiting travel and investment in real estate, and access to high quality education and healthcare systems…
>
> The transparency aspects of targeted sanctions may involve publicly identifying a 'watchlist' of individuals being considered for sanctioning, as well as publishing a list of those who have been sanctioned, including the reasons for the sanctions. This combination serves to 'name and shame' and can also alert banks or other institutions that may otherwise do business with or facilitate transactions of sanctioned individuals.[62]

At this point, it is important to note that the court has considered that intellectual property – including papers or notes – is an "asset" under Australian sanctions law.[63] Therefore, any designated entity would not be permitted to participate in research programs with Australian universities, where the handling of intellectual property would constitute "dealing" with an "asset" in a manner that contravenes a sanction law.

This should be a matter clearly articulated to the Government in the Committee's report, even if the other recommendations relating to bolstering Australian research security are not adopted, as this ought to turn the Government's mind to the inherent power for protecting our research ecosystem that is present in Australian sanctions law.

Recommendation 5: The Committee should recommend that the Government issue (through DFAT) more specific and updated guidance, especially to the higher education sector, about the implications of supplying intellectual property as an "asset" to a designated person or entity.

Curiously, Australian sanctions law does not *prima facie* prohibit a natural person who is designated or declared under Australian sanctions law from being a director and/or holding corporate office in Australia. Although one may take it as read that corporate social responsibility may militate towards not engaging a person subject to such sanctions,[64] there is no specific provision which does so

[60] Reg 12 to 16 (inclusive) are declared to be 'sanction laws' for the purposes of s 6 of the Act by the *Autonomous Sanctions (Sanction Law) Declaration 2012* (Cth). That means that contravention of any of those Regulations is (subject to proof of the relevant fault elements) an offence under s 16 of the Act.

[61] Being 'an asset or property of any kind, whether tangible or intangible, movable or immovable' and 'a legal document or instrument in any form (including electronic or digital) evidencing title to, or interest in, such an asset or such property': *Autonomous Sanctions Act 2011* (Cth), s 4.

[62] Committee Review Report, [3.9]-[3.10].

[63] The case brought by the applicant in *Deripaska* clearly contemplated that the knowledge of an Australian lawyer would be an "asset" under sanctions law, and His Honour Kennett J agreed. Though the statement was obiter, it was not contested and was not the subject of any appeal: *Deripaska v Minister for Foreign Affairs* [2024] FCA 62, [41].

[64] Indeed, the Federal Court would likely support that position, given that recent decisions have imposed a low bar on how 'sanctioned supply' to related corporate entities might circumvent Australian sanctions law: *Alumina and Bauxite Company Ltd v Queensland Alumina Ltd* [2024] FCA 43; upheld on appeal, *Alumina and Bauxite Company Ltd v Queensland Alumina Ltd* [2024] FCAFC 142.

automatically.[65] That position may be contrasted strongly with UK sanctions law, whereby a natural person who is subject to sanctions may be prohibited from holding directorships in a company if the regulations provide for it.[66]

Recommendation 6: That the Committee recommend to Government that:

- Section 206B of the *Corporations Act 2001* (Cth) be amended such that any natural person who is the subject of a designation under Australia's autonomous sanctions regime be "automatically disqualified" as a person who may permissibly manage or direct Australian corporations; or
- In the alternate, the *Autonomous Sanctions Act 2011* (Cth) be amended to include a power for the Minister to sanction a designated person as no longer being a fit and proper person to be a director of an Australian company, and to report that matter to ASIC.

Unnecessary limitations on thematic sanctions

Under Australian sanctions law, thematic sanctions may only involve "Targeted Financial Sanctions" and bans on travelling to, entering or remaining in Australia.[67] The Explanatory Memorandum to the Magnitsky Act makes clear that this was always an intended consequence of the passage of the Magnitsky reforms.[68] Again, referring to both US and UK autonomous sanctioning regimes, persons and entities may be designated as persons or entities "of concern" for reasons of foreign or domestic policy, security or other similar grounds.

Sanctions available for thematic sanctions under *Autonomous Sanctions Act 2011* (Cth)	Sanctions available for thematic sanctions under *Sanctions and Money Laundering Act 2018* (UK)	Sanctions available for thematic sanctions under EAR (15 CFR 730-744).
• Designated person or entity • Travel ban	• Designated person or entity • Trade sanctions, including arms embargoes and other trade restrictions • Financial sanctions, including asset freezes • Immigration sanctions, known as travel bans • Aircraft and shipping sanctions, including de-registering aircraft and ships	• Designated person or entity • Trade sanctions, including arms embargoes and other trade restrictions • Financial sanctions, including asset freezes • Immigration sanctions, known as travel bans

Table 2: Comparison of sanctions available under Australian, UK and US law

[65] I note that a director disqualification under UK sanctions law would not automatically operate in Australia, as a Regulation is not 'an order made by a court of a foreign jurisdiction that is in force': *Corporations Act 2001* (Cth) s 206B(6), and would need to be the subject of proceedings brought on by ASIC: *Corporations Act 2001* (Cth) s 206EAA(1).

[66] *Company Directors Disqualification Act 1986* (UK) s 11A; *Company Directors Disqualification (Northern Ireland) Order 2002* (UK) art 15A.

[67] *Autonomous Sanctions Regulation 2011* (Cth) rr 6A(1), (2), (4), (5), (8) and (9).

[68] Explanatory Memorandum to the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Bill 2021, [1], [24] and [26].

However, there appears to be no apparent or valid reason why thematic sanctions should be so limited in relation to their scope and application, especially where the Minister as decision-maker is vested with the discretion to fully consider what (if any) sanctions ought to be applied. Not amending this provision will mean Australia is out of step with its international allies and cannot bring the full weight of potential sanctions in support of Australian foreign policy.

Recommendation 7: The Committee should recommend that the Government amend Regulation 6A of the *Autonomous Sanctions Regulation 2011* (Cth) to include provisions for the Minister to impose trade and/or financial sanctions in the course of considering a thematic sanction.

Applications for sanctions

Recommendation 15 of the Committee's previous review stipulated that the 'decision maker should be able to receive nominations from any source'.[69] In the Government's response to the Committee inquiry, this recommendation was "Agreed", with the government stating that 'any individual or organisation can make representations to the Government regarding potential sanctions targets'.[70]

However, if this is still the Australian Government's position, it does not appear to accord with the current practice of DFAT. A review of the Department's website (https://www.dfat.gov.au/international-relations/security/sanctions) does not advise members of the public that this option is available. Nor does the Department published any guidance on how any individual or organisation might apply for a sanction to be imposed on a person or entity. Finally, there is no broader information on the listing process (dealt with below) which would inform an applicant for a sanction on what (if any) communication they can expect to receive from either the Minister or DFAT if they choose to seek a sanction against a person or entity.

Transparency and accountability remain a key hallmark of the Australian sanctions regime (subject only to limited exemptions to protect Australian national security or foreign policy considerations). As was said by the Committee in the last Review, '[i]mplementation of the sanctions will also be easier if the sanctions are public and widely known… the Minister responsible for nominating sanctions targets should encourage visibility of the process and outcomes'.[71] For those reasons, the Government should be encouraged to provide additional information to applicants on how sanction targets might be nominated for the Minister's consideration (and what they can expect from that process).

Recommendation 8: The Committee should recommend that the Government publish information on the DFAT website relating to sanctions that:

a.) Any member of the public and/or entity may apply to the Minister for a natural person or entity to be the subject of an autonomous sanction; and
b.) The process/es and procedure/es for requesting that a natural person or entity be the subject of an autonomous sanction.

Oversight, review and de-listing

The existing Magnitsky Act includes a requirement for the Foreign Minister to both 'consult the Attorney - General and obtain the Attorney - General's agreement in writing to the making of the

[69] Committee Review Report, [5.60].
[70] Australian Government Response, 9.
[71] Committee Review Report, [5.87]-[5.90].

instrument' (the "approval requirement")[72] and to 'consult such other Ministers as the Minister considers appropriate' (the "consultation requirement").[73] Both the approval requirement and the consultation requirement are important safeguards that are required to limit the potential implications of, and adverse consequences to, designated persons or entities when sanctions are proposed. The requirement to seek the approval of the Attorney-General as First Law Officer remains appropriate and necessary. Further, there may be a need to discuss the proposal with Ministers of other portfolios, i.e., cybersecurity, defence, home affairs or education, to ensure that the Foreign Minister has been appraised of the potential implications of any proposed thematic sanction.

Recommendation 9: That the Committee recommend to Government that the *Autonomous Sanctions Act 2011* (Cth) retain the approval requirement for thematic sanctions to be approved by the Attorney-General.

Recommendation 10: That the Committee recommend to Government that the *Autonomous Sanctions Act 2011* (Cth) retain the consultation requirement for "such other Ministers as is deemed appropriate" to be consulted prior to enactment of thematic sanctions.

The process for de-listing is not apparent in either the Act or Regulations (presumably because the making of a designation or declaration may be repealed, rescinded, revoked, amended, or varied by the Minister at any time[74]). DFAT's website suggests that a request may be made via the ASO at any time by a designated person or entity for de-listing, whereupon presumably it would come before the Minister and the applicant informed of the outcome.

This is not an ideal situation. Persons who have been the subject of a designation or declaration face substantial and sustained interference with their human rights and freedoms by virtue of a fiat of the Executive. Whilst I concur with the Government's findings after the previous Committee's review that 'it is essential that potential targets of sanctions do not receive advance notice of potential sanctions',[75] I do agree that '[c]lear criteria and a methodology for listing and de-listing sanctions would ensure transparency and accountability for Government'.[76] Neither the Minister or DFAT should be excused from properly and transparently communicating how the listing and de-listing process operates.

Recommendation 11: The Committee should recommend that the Government publish information on the DFAT website about the process of listing and de-listing, as well as providing resources for persons or entities applying for de-listing.

There is also no specific ground of review in either the Act or the Regulations, for review of either the making of Regulations by the Governor-General (either for country-specific sanctions or thematic sanctions) nor the Minister's subsequent designations or declarations. Instead, reviews have largely been handled by way of the inherent review jurisdiction of the Federal court system.[77] Regulations

[72] *Autonomous Sanctions Act 2011* (Cth), ss 10(4)(c) and 10(5)(c).
[73] Ibid, ss 10(4)(d) and 10(5)(d).
[74] *Acts Interpretation Act 1901* (Cth), s 33(3).
[75] Australian Government Response, 10.
[76] Committee Review Report, [2.64].
[77] Bestowed by s 5(1) of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and ss 39B(1) and (1A)(c) of the *Judiciary Act 1903* (Cth). See also the 'entrenched minimum provision of judicial review' conferred by

made by the Governor-General are also 'legislative instruments' and so may be subject to a motion to disallow in Parliament, though this is rarely done.[78]

The most prominent judicial review of Australian sanctions law occurred in *Abramov*.[79] There, Alexander Abramov was a Russian national with significant shareholdings in Russian entities involved in steel and coal production. He was then designated by then-Foreign Minister Marise Payne.[80] Mr Abramov succeeded on only one ground, that being that the Minister's conduct in designated him 'amounted to a constructive failure to exercise jurisdiction, because the Minister failed to apply the correct test or misunderstood the nature of the power conferred on her'.[81]

That said, a nearly identical administrative review challenge failed in *Deripaska*, after the applicant failed to prove that the Minister had inadequately considered any of the material before her or exercised the sanctions powers in any improper manner.[82] His Honour Kennett J explicitly identified in his reasons that:

> It will be apparent that I have come to a different conclusion, in the context of this case, about what the somewhat convoluted language of the Recommendation would have conveyed to the Minister and the significance of the Ministerial Submission having included discussion of matters that were irrelevant to whether the applicant met the criteria in item 6A.[83]

Given that two learned Judges of the Federal court system have reached wildly divergent opinions about the scope of discretion available to the Minister in making designations and determinations under the *Autonomous Sanctions Act 2011* (Cth), there is some validity to suggesting a specific ground of review in that Act might better guide the operation of the sanctions regime. Alternately, the Regulations may provide specific criteria for the Minister to consider in conducting an internal review of a designation or declaration decision. Of course, this will not oust the inherent jurisdiction in the Federal court system but may provide greater clarity and transparency on the Australian regime.

Recommendation 12: The Committee should recommend that the Government consider amending the *Autonomous Sanctions Act 2011* (Cth) to provide for a limited merits review process of designation and/or determination decisions.

Recommendation 13: If that Recommendation is not accepted, the Committee should recommend that the Government consider amending the *Autonomous Sanctions Regulations 2011* (Cth) to provide specific criteria for the Minister to conduct an internal review of designation and/or determination decisions (which must, as a minimum, specify that the Minister personally undertake such reviews).

---

section 75(v) of the *Constitution*: *Plaintiff S157/2002 v Commonwealth* [2003] HCA 2; 211 CLR 476 at [103] (Gaudron, McHugh, Gummow, Kirby and Hayne JJ).

[78] *Legislation Act 2003* (Cth), ss 8(5), 10(1)(a) and 42(1).

[79] *Alexander Abramov v Minister for Foreign Affairs (No 2)* [2023] FCA 1099.

[80] *Autonomous Sanctions (Designated Persons and Entities and Declared Persons – Russia and Ukraine) List 2014* (Cth), as amended by the *Autonomous Sanctions (Designated Persons and Entities and Declared Persons — Russia and Ukraine) Amendment (No 11) Instrument 2022* (Cth).

[81] *Alexander Abramov v Minister for Foreign Affairs (No 2)* [2023] FCA 1099, [108], [112] and [123].

[82] *Deripaska v Minister for Foreign Affairs* [2024] FCA 62.

[83] Ibid, [143].

Conclusion

Thank you for the opportunity to make this submission. I look forward to hearing the result of the Committee's review of the Magnitsky Act.

Dr Brendan Walker-Munro

brendan.walker-munro@scu.edu.au